

RENÉ HUMBERTO MÁRQUEZ ARCILA

Auditoría forense

AUDITORÍA



Instituto Mexicano de
Contadores Públicos

Derechos reservados

©2018 Instituto Mexicano de Contadores Públicos, A.C.

Bosque de Tabachines 44 Fracc. Bosques de las Lomas 11700 Ciudad de México

www.imcp.org.mx

©2018 René Humberto Márquez Arcila

AUDITORÍA FORENSE

ISBN 978-607-8552-63-4

1a edición, abril 2018

EDITORIAL

Azucena GarcíaNares Gerencia Editorial

Norma Berenice San Martín López Coordinación Editorial

Jorge Alejandro Medina Arriaga Coordinación de Diseño y portada

Jesús Antonio Díaz de León Castañeda Diagramación

Antonio Cardoso Zúñiga Corrección de estilo

José de Jesús González Gutiérrez Analista de producción

Shutterstock® Images Banco de imágenes

La transformación a libro electrónico del presente título fue realizada por **Capture®**.

Todos los derechos reservados. Ninguna parte de esta obra debe ser reproducida, almacenada en algún sistema de recuperación o transmitida de cualquier forma o por cualquier medio, ya sea electrónico, mecánico, fotocopiado o de filmación, sin el permiso previo y por escrito del editor.

Publicado en México/Published in Mexico

Este libro se lo dedico a mis hijos René y Renata, y a la compañera de todas mis aventuras,
mi amada esposa Anel.

René, el soñador que lucha día con día para conseguir sus metas; joven audaz
que conquistará todas las montañas que se proponga.

Renata mi princesa, su carácter fuerte domina su futuro inquebrantable,
hermosa navegará los océanos disfrutando sus rebeldías.

Anel, gracias por tu paciencia, comprensión y amor.

A mi familia Márquez Arcila, aquí estaré siempre a su lado, muy orgulloso
de ser la persona en la que me he convertido.

A Dios, gracias por permitirme vivir.

Doctor en Análisis Estratégico y Desarrollo Sustentable por la Universidad Anáhuac Mayab, Maestro en Finanzas y Contador Público por la Universidad Autónoma de Yucatán, Contador Público Certificado y Certificación en la Disciplina de Auditoría y Contabilidad Gubernamental por el Instituto Mexicano de Contadores Públicos, Certificado como Examinador de Fraude por la Asociación de Examinadores de Fraude, Certificado en Aseguramiento y Gestión de Riesgos por el Instituto de Auditores Internos y Certificación en Fiscalización Pública por la ASOFIS y el IMAI.

Actualmente es Vicepresidente del Sector Gubernamental del Instituto Mexicano de Contadores Públicos por el periodo 2107-2019.

Autor de los libros: *Fiscalización y rendición de cuentas* (2013) y *Auditoría de desempeño* (2014).



En el Instituto Mexicano de Contadores Públicos (IMCP) estamos a la vanguardia en temas que hoy la profesión requiere conocer, ya sean a nivel internacional o los que México necesita para seguir avanzando como país.

El sistema nacional anticorrupción, el sistema nacional de fiscalización y el sistema nacional de transparencia son los ejes sobre los que descansará el combate a la corrupción.

En este entorno de mejorar y establecer un nuevo marco jurídico para la fiscalización y rendición de cuentas en México, la investigación y sustanciación, que permitirán al auditor recopilar evidencia más sólida, cobran especial relevancia; por ello, este libro de auditoría forense coadyuvará para dar conocer y profesionalizar el tema en las universidades y apoyar a los profesionales que deseen desempeñarse como auditores forenses.

Asimismo, los grandes grupos empresariales tienen avances significativos en auditoría forense, y con este libro el conocimiento llegará a las medianas y pequeñas empresas; es decir, el tema empresarial con la entrada en vigor de las reformas a la ley de responsabilidades administrativas otorga nuevas obligaciones a los empresarios que contraten recursos públicos, por lo que la auditoría forense será importante en la investigación y disuasión del fraude.

La obra servirá también para impulsar esta área profesional en Latinoamérica, ya que, entre otros temas, compartimos nuestras mejores prácticas en temas de auditoría de desempeño y evaluación de desempeño, ley de disciplina financiera, ley general de contabilidad gubernamental y presupuesto basado en resultados.

Sin lugar a duda, apoyar obras como esta, que contribuyen al fortalecimiento de la profesión, también respalda los objetivos de este Comité Ejecutivo Nacional al posicionar al IMCP como líder de la Contaduría Pública ante todos los sectores de la economía nacional y los correspondientes internacionales, además de brindar un servicio a sus asociados, organizaciones públicas y privadas, y al público en general, basado en la excelencia de su liderazgo.

C.P.C. José Besil Bardawil
Presidente del Comité Ejecutivo Nacional
2017-2018 IMCP

CONTENIDO

Introducción

Capítulo 1. ¿Qué es la auditoría forense?

- 1.1 Definición de auditoría forense
- 1.2 Esquemas de fraude corporativo
 - 1.2.1 Corrupción
- 1.3 Comprensión y análisis del fraude
 - 1.3.1 Teoría del fraude
 - 1.3.2 Indicadores de la ocurrencia de fraude (banderas rojas)
 - 1.3.3 Perfil del defraudador
- 1.4 El fraude en las organizaciones y el impacto de la auditoría forense
 - 1.4.1 Evaluación de riesgos de fraude y establecimiento de controles
 - 1.4.2 Responsabilidades del personal en la prevención y detección de fraude
 - 1.4.3 Métodos de detección de fraude
 - 1.4.4 Política de ética organizacional y política antifraude
- 1.5 Evaluación del riesgo de fraude
 - 1.5.1 Formas de enfrentar un fraude
 - 1.5.2 Consideraciones acerca de la oportunidad de fraude
 - 1.5.3 La auditoría forense
 - 1.5.4 Responsabilidad de los auditores ante el fraude
 - 1.5.5 Teoría del control de fraude
 - 1.5.6 Programas antifraude
 - 1.5.7 Importancia del control interno
 - 1.5.8 Reporte de auditoría forense
 - 1.5.9 Diferencia entre auditoría forense e investigación de fraude

Anexos

- 1.1 ¿Qué es la auditoría forense?
- 1.2 Nuevas formas de fraude y sus características
- 1.3 Comprensión y análisis del fraude ocupacional
- 1.4 Prevención, disuasión y detección de fraude
- 1.4 Prevención, disuasión y detección de fraude

Capítulo 2. Metodología de auditoría forense

- 2.1 Metodología de auditoría forense
 - 2.1.1 Evaluación preliminar
 - 2.1.2 Planeación
 - 2.1.3 Ejecución
 - 2.1.4 Informe
 - 2.1.5 Monitoreo
 - 2.1.6 Proceso legal
- 2.2 Casos prácticos
 - 2.2.1 Caso Supermercado Transnacional
 - 2.2.2 Caso de la empresa Ingeniería Marina
 - 2.2.3 Caso Lavado de dinero: Cyber criminals-dinero digital
 - 2.2.4 Caso de la empresa en óptica e imagen

Anexos

- 2.1 Procedimientos analíticos 1
- 2.2 Procedimientos analíticos 2
- 2.3 Técnicas de análisis asistidas por computadora
- 2.4 Entrevista e interrogatorio

Capítulo 3. ¿Cómo crear un departamento de auditoría forense?

3.1 El departamento de auditoría forense

3.2 Perfil del auditor forense

3.3 Asociaciones profesionales especializadas en fraude

3.3.1 Asociación de Examinadores de Fraude Certificados (ACFE)

3.3.2 Universidad Americana de Examinadores Forenses

3.3.3 Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS)

3.3.4 Sociedad de Cumplimiento Corporativo y Ética (SCCE)

3.3.5 Sociedad Americana para la Seguridad Industrial (American Society for Industrial Security, ASIS)

3.4 Desarrollo profesional continuo del auditor forense

3.5 Laboratorio forense: tecnología avanzada para el desempeño de la profesión

3.5.1 Descripción del laboratorio forense

3.5.2 Objetivos del laboratorio forense

3.5.3 Estructura y funciones del laboratorio forense

3.6 Visión internacional del fraude

3.7 El fraude en México y sus implicaciones

3.8 Marco legal internacional contra el fraude

3.9 Importancia de las certificaciones profesionales en el marco de crear perfiles profesionales para combatir el fraude

Anexos

3.1 Ejemplo de funciones del departamento de auditoría forense

3.2 Ejemplo de perfil del auditor forense

3.3 Fraude en México

Conclusiones

Bibliografía

Resumen de gráficos e ilustraciones

Los fraudes corporativos ocurridos durante los años noventa y dos mil, generaron gran preocupación acerca de si las organizaciones y sus sistemas de control y detección de fraudes eran realmente eficaces.

Diversos escándalos a nivel internacional como los casos de: Enron, WorldCom y Parmalat, entre otros, crearon la necesidad de revisar el marco de normas y leyes con el fin de regular de una mejor manera a las empresas, al gobierno, a las firmas de auditoría externa e interna, a la bolsa de valores y a otros órganos económicos y de supervisión.

En los Estados Unidos de América, la Ley Sarbanes-Oxley surge a partir de la necesidad de supervisar de una forma óptima a las empresas que cotizan en la bolsa de valores; de igual manera, alrededor del mundo se diseñaron leyes para el combate a la corrupción, soborno y prácticas de extorsión como, por ejemplo, la Ley Anticorrupción (*Anti-Corruption Act*, 2011) y la Ley de Prácticas Corruptas en el Extranjero (*Foreign Corrupt Practices Act*, 1997) en Estados Unidos de América; la Ley Antisoborno (*Bribery Act*, 2007) en Reino Unido, así como el Sistema Nacional Anticorrupción (2016) en México, son algunos de los ejemplos de legislación aplicable a los actos delictivos relacionados con el fraude y la corrupción.

Asimismo, el interés por la prevención y detección oportuna del fraude no sólo ha sido de los gobiernos y organismos internacionales por medio de sus legislaciones, sino también por organizaciones profesionales que, mediante la creación de comités y comisiones, han creado normas y marcos regulatorios para las actividades financieras del sector empresarial y gubernamental para combatir el fraude.

Ejemplo de esto fue la creación del Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO) en 1985, patrocinada por cinco organizaciones representativas en Estados Unidos en el campo de contabilidad, finanzas y auditoría interna: La Asociación de Contadores Públicos Norteamericanos (AAA), el Instituto Norteamericano de Contadores Públicos Certificados (AICPA), la Asociación Internacional de Ejecutivos de Finanzas (FEI), el Instituto de Auditores Internos (IIA) y el Instituto de Contadores Empresariales (IMA).

COSO tiene como finalidad la creación y actualización de marcos y guías generales sobre el control interno, la gestión del riesgo empresarial y la disuasión del fraude, con el objetivo de mejorar el control organizacional, la supervisión y la prevención de errores, omisiones o fraude en las organizaciones. Estos marcos de control permiten la identificación de factores que originan la presentación de información financiera falsa o fraudulenta.

Asimismo, estas organizaciones han creado normas de auditoría y de presentación de información financiera que colaboran con este mismo propósito. Las NIA (Normas Internacionales de Auditoría) emitidas por la Federación Internacional de Contadores (IFAC), así como las NIIF (Normas de Información Financiera) emitidas por el Consejo Internacional de Normas de Contabilidad (IASB) son regulaciones que se utilizan a nivel internacional, con el fin de contar con lineamientos comunes de contabilidad y auditoría, facilitando la prevención y detección de fraude en estados financieros.

Las normas del INTOSAI (Organización Internacional de las Entidades Fiscalizadoras Superiores) son las siguientes: ISSAI 100 —Principios fundamentales de auditoría del sector público—, ISSAI 200 —Principios fundamentales de auditoría financiera—, ISSAI 300 —Principios fundamentales de auditoría de desempeño—, ISSAI 400 —Principios fundamentales de auditoría de cumplimiento—.

Las organizaciones que trabajan en la prevención, detección y disuasión del fraude convergen en considerar a la ética como eje central para ello. La existencia de un código de ética que establezca la postura de la alta dirección hacia los actos de ilegalidad y fraude, es un requisito indispensable en un programa de prevención y disuasión del fraude.

Las organizaciones con cultura antifraude deben contar con un proceso establecido para gestionar los riesgos existentes y, de manera especial, el fraude. Lo anterior debido a que el impacto de este último significa la pérdida de activos valiosos para la organización, además de un daño irreparable a su reputación.

Las instituciones especializadas en el estudio del fraude han desarrollado mediciones que permiten establecer un sistema de fraude en la organización, así como mecanismos para prevenirlo, detectarlo y disuadirlo. La prevención es el mejor enfoque para el fraude, implica el establecimiento de controles preventivos y directivos como comunicación y capacitación interna sobre fraude, políticas que promuevan el comportamiento correcto, así como sistemas de apoyo para los miembros de la organización en situaciones que se convierten en vulnerables a la comisión de delitos.

En la actualidad, los marcos legales requieren de procesos jurídicos de mayor complejidad, por lo que es necesario utilizar metodologías de auditoría forense y técnicas confiables basadas en herramientas de alta tecnología, que permitan el análisis de gran cantidad de información y con eficiencia del tiempo y recursos. Asimismo, que permitan la obtención, cuidado y custodia de la evidencia.

Hoy en día, para las organizaciones tanto del sector público como privado es de gran valor contar con profesionales certificados como auditores forenses (CFE), que puedan proteger a la organización sobre conductas de fraude, así como coadyuvar en el establecimiento de una cultura ética y crear políticas antifraude efectivas.

Capítulo 1

¿Qué es la auditoría forense?



¿Qué es la auditoría forense?

1.1 Definición de auditoría forense

El concepto auditoría forense está compuesto por dos términos que definen la naturaleza de su función: “auditoría”, que de acuerdo con el diccionario de la lengua española se refiere a la revisión de la contabilidad de una empresa u organización para garantizar la veracidad y regularización de las cuentas y elaborar un dictamen sobre la calidad de la gestión, y “forense”, que proviene del latín *forensis* y significa “público y manifiesto” o “perteneiente al foro”; a su vez, “forensis” se deriva de *forum*, que significa “foro”, “plaza pública”, “plaza de mercado” o “lugar al aire libre”.

El término forense proviene de la antigua Roma, en donde las actividades políticas, religiosas, comerciales y jurídicas se realizaban en la plaza principal; en dichos foros también se trataban los negocios públicos y se celebraban los juicios; por ello cuando una profesión sirve de soporte, asesoría o apoyo a la justicia para que se juzgue a la persona que cometió un delito se le denomina “forense”, tal es el caso de disciplinas como la medicina, la grafoscopia, la psicología, la antropología, la genética, la química y la auditoría, entre otras.

La auditoría forense es una disciplina que sirve como asesor experto a quienes imparten justicia, en la investigación y obtención de evidencia, acerca de la existencia de un delito financiero o relacionado con los activos de la organización. La función de la auditoría forense consiste en evaluar los procesos de la organización evaluando excepciones, irregularidades contables y patrones de conducta que pueden considerarse anormales; esto mediante un análisis lógico y sistemático que les permite obtener evidencia legal de hechos presuntamente delictivos que podrían dañar el interés público o privado.

Asimismo, esta disciplina debe contestar a las siguientes preguntas: ¿qué ocurrió?, ¿cómo ocurrió?, y ¿quién es responsable por lo que ocurrió? Para esto, se requiere la utilización de técnicas para obtener información más precisa y específica, así como para realizar un análisis de mayor alcance que el de las técnicas de auditoría tradicionales.

La auditoría forense puede ser correctiva, enfocándose en los fraudes que ya han sido cometidos, y también preventiva evaluando las medidas tomadas por la dirección u otros cuerpos de gobierno responsables, para prevenir y predecir situaciones indeseables relacionados con el fraude; investigar aquellos hechos que se le encomienden como sospechosos de actos delictivos, entre otras funciones relacionadas con la prevención.

La organización es la que determina el rango de funciones o atribuciones de la auditoría forense, además de las mencionadas anteriormente también puede cumplir un rol de asesoría, capacitación y soporte durante litigios, valiéndose de diversas técnicas para la obtención de información.

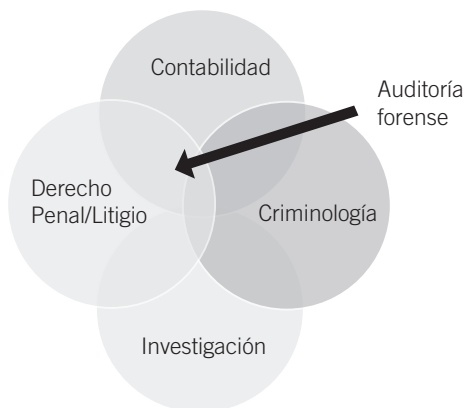
Algunas de las principales áreas de competencia son:



Fuente: Elaborado por el autor.

Para llevar a cabo sus funciones de manera proactiva e interdisciplinaria, la auditoría forense integra conocimientos de contabilidad, criminología, cómputo forense, investigación y derecho penal/litigio para la investigación de amplio rango de problemas futuros del negocio. La investigación incluye la examinación del fraude, revisiones de debida diligencia, evaluación del riesgo, detección de declaraciones falsas en los estados financieros, crímenes cibernéticos, transferencias de dinero ilegales (G. Stevenson Smith, 2009).

Ilustración 1. Disciplinas relacionadas con la auditoría forense



Fuente: G. Stevenson Smith, 2009.

La auditoría forense se diferencia de otros tipos de auditoría al contar con un esquema metodológico-flexible; las fases, técnicas, perfiles profesionales y procedimientos que se utilizan varían, dependiendo de las características del fraude; sin embargo, mantiene un enfoque de auditoría legal que permite obtener evidencia confiable.

Algunas de las principales diferencias de la auditoría forense con otros tipos de auditoría similares se presentan a continuación:

Ilustración 2. Comparativo entre auditoría forense y otras disciplinas

Característica	Auditoría financiera	Investigación/Examinación de fraude	Auditoría forense
Perspectiva de tiempo	Histórico	Histórico	Futuro e histórico
Enfoque principal	Periódico	Reactivo	Proactivo y reactivo
Objeto de investigación	Estrecho	Estrecho	Amplio alcance
Producto de trabajo	Opinión de auditoría	Reporte del caso de fraude	Reporte de auditoría forense
Principal responsabilidad	La organización y el público	La parte defraudada	La organización, director o un tercero
Su guía es:	Basado en reglas rígidas	Basado en principios bajo las reglas de auditoría	Basado en principios
Propósito del reporte	Asegurar que se siguen las normas	Se identifica un perpetrador del fraude y las causas	Evaluación del riesgo de fraude y servicios estratégicos. Se identifican fraudes potenciales y existentes

Fuente: Elaborado por el autor.

La auditoría forense se diferencia de otros enfoques de auditoría en su característica preventiva, ya que mantiene un programa de aseguramiento constante del riesgo de fraude y sugiere medidas de control; detecta fraudes que deberán ser investigados a profundidad y ser llevados a estancias legales en su caso; considerando al fraude como la representación equivocada e intencional de hechos financieros o malversación de activos de naturaleza material.

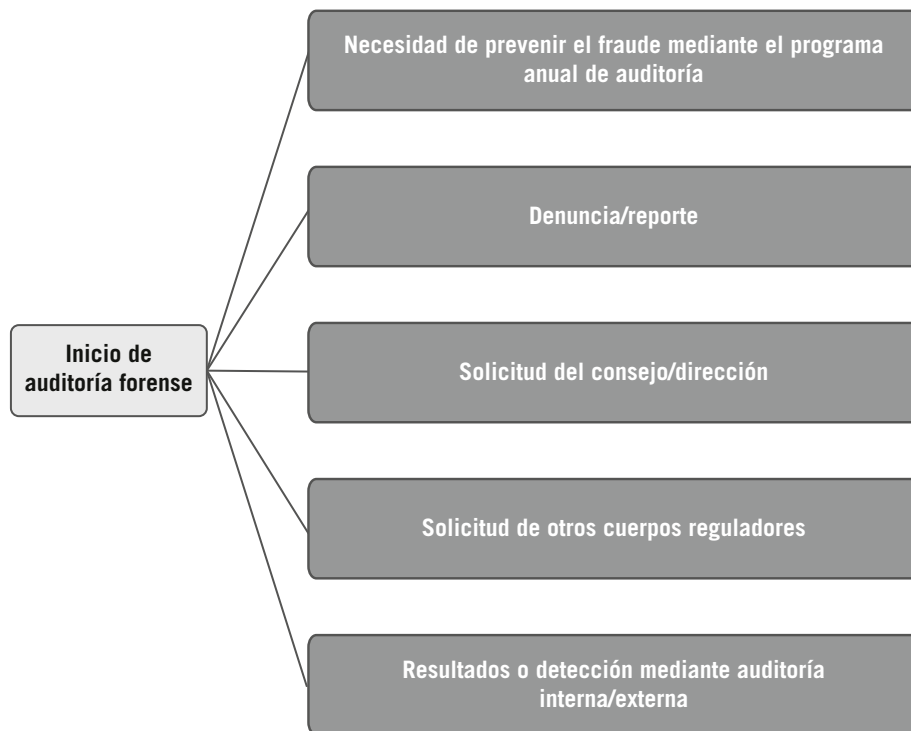
El tiempo en que se realiza la auditoría forense define el enfoque que deberá utilizarse, esto de acuerdo con las necesidades de la organización. Existen dos enfoques que la caracterizan y que definirán el plan de trabajo o estrategias que la auditoría forense desempeñe en la organización:

- Enfoque preventivo.** Orientado a realizar auditorías contempladas en el plan anual de auditorías con el propósito de prevenir y disuadir irregularidades e indicadores de la existencia de un fraude. Este enfoque también incluye la creación e implementación de programas y controles antifraude, esquemas de alerta temprana de irregularidades y sistemas de administración de denuncias.
- Enfoque detectivo.** Este enfoque se utiliza cuando existen indicios o información a partir de la cual se puede presumir la existencia de un delito; se caracteriza principalmente por utilizar técnicas enfocadas a obtener evidencia que pruebe el hecho de manera legal. Está orientado a identificar la existencia de fraudes mediante una profunda investigación, llegando a establecer entre otros aspectos los siguientes:

- Determinar la cuantía del fraude.
- Efectos directos e indirectos.
- Posible tipificación.
- Presuntos autores.
- Cómplices y encubridores.

El enfoque de auditoría utilizado depende de la causa u origen de la auditoría realizada; por ejemplo la alta dirección percibe un alto riesgo en un área en particular, debido a su nueva creación y requiere asegurarse del cumplimiento de las normas, por lo que se realizará una auditoría forense preventiva. Por el contrario, en caso de tener indicios o evidencias de la posible existencia de un ilícito, deberá realizarse una auditoría con enfoque detectivo.

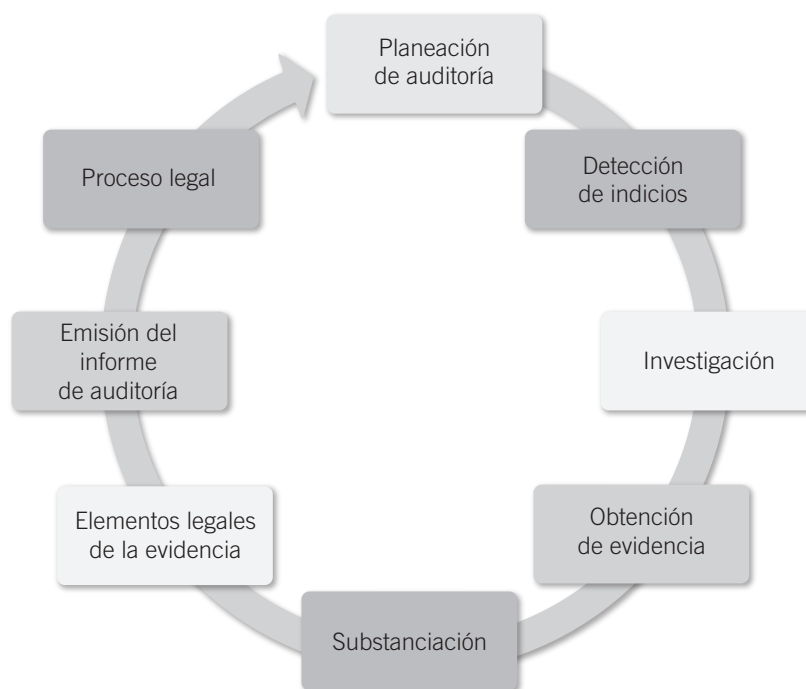
Es probable que la auditoría forense se origine a raíz de alguno de los siguientes motivos:



Fuente: Elaborado por el autor.

La evaluación de control interno ayuda a identificar a los posibles responsables de las operaciones fraudulentas, los presuntos involucrados que pueden ser de la misma organización o con terceros relacionados y evaluación del riesgo aplicada a la organización, los resultados generados de dicha evaluación otorgarán la pauta para el diseño de procedimientos de auditoría que ofrezcan certidumbre razonable para la detección de las distorsiones producidas por fraude o error, que tengan un efecto material en el conjunto de operaciones, recursos y en los estados financieros con lo que se inicia la auditoría forense, así como las características y naturaleza de los bienes, personas o procesos a auditar deberán considerarse durante la planeación. Es de principal relevancia la capacidad y pericia del auditor, dado que por la naturaleza del trabajo se requiere la utilización del juicio profesional durante todo el proceso; mismo que debe estar respaldado por una amplia experiencia que facilite la toma de decisiones relacionadas con la metodología, presupuesto y ética, entre otros aspectos. Se sugiere el proceso de una auditoría forense de la siguiente manera:

Ilustración 3. Proceso de la auditoría forense



Fuente: Elaborado por el autor.

La auditoría forense tiene como objeto de estudio los posibles ilícitos relacionados con los bienes de la organización; cometidos dentro o fuera de ésta y afectando sus intereses y permanencia.

En el sector financiero el fraude es uno de los ilícitos más comunes, ocasiona pérdidas anuales millonarias a las organizaciones en todo el mundo; este fenómeno económico y social es definido por el Instituto de Auditores Internos como: cualquier acto ilegal caracterizado por engaño, ocultación o violación de confianza, mismo que no implica la aplicación de amenaza de violencia o de fuerza física. Otra definición de fraude proveniente de la publicación “Gestión del riesgo de fraude en las organizaciones. Una guía práctica”; auspiciada por el IIA, el AICPA y la ACFE, indica que: “fraude es cualquier acción u omisión intencional diseñada para engañar a otros, con el resultado de que la víctima sufre una pérdida y/o que el perpetrador logra una ganancia”.

El delito de fraude es perpetrado por individuos y organizaciones para obtener dinero, bienes o servicios, así como para evitar pagos y pérdidas de servicios, o para asegurarse ventajas personales o de negocio.

La comprensión de cómo se lleva a cabo este delito es fundamental para las organizaciones, ya que se ha convertido en una de las principales causas de pérdida financiera y reputacional en la actualidad. El análisis estadístico de los datos recopilados en organizaciones sobre los casos de fraude detectados, proporcionan directrices acerca de la manera en que deben estar diseñados los planes y estrategias para prevenir, detectar y disuadir el fraude.

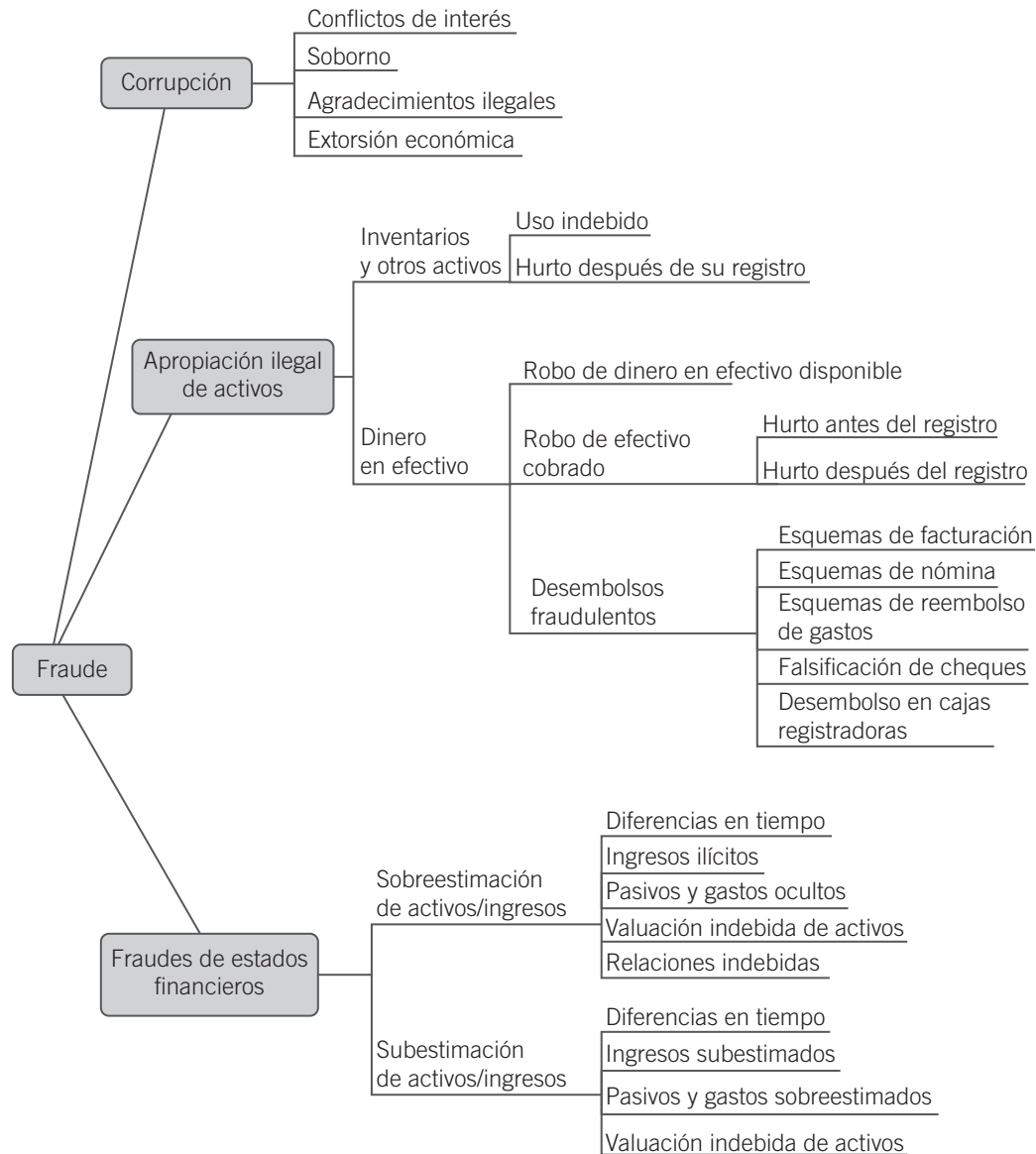
El término fraude presenta una definición bastante amplia e incluye diversos tipos de delitos en sí mismo, por lo que para efectos de este capítulo se presenta de manera más amplia el fraude de tipo corporativo; que es considerado como toda conducta de engaño o violación de confianza que busca obtener un beneficio perpetrado por miembros de la organización en contra o en favor de la misma. Lo anterior no implica solamente a organizaciones del sector privado, sino a toda organización que realiza una actividad productiva y administra recursos financieros u otros bienes.

La auditoría forense es reconocida internacionalmente como un conjunto de técnicas efectivas para la prevención e identificación de actos irregulares de fraude y corrupción.

1.2 Esquemas de fraude corporativo

La Asociación de Examinadores de Fraude Certificados (ACFE) ofrece la clasificación más aceptada en el mundo de fraudes corporativos. A continuación se presenta una descripción de cada uno de estos esquemas y sus características, mismas que son importantes de considerar al realizar una auditoría forense, ya que se emplean diversos métodos y técnicas de acuerdo con el esquema que se presenta.

Ilustración 4. Árbol del fraude / Clasificación esquemas de fraude



Fuente: ACFE.

1.2.1 Corrupción

El esquema de fraude por corrupción es aquel en donde los empleados de una empresa utilizan de forma indebida sus influencias para obtener un beneficio personal frecuentemente fuera de los libros contables; lo que significa que hay pocas pruebas financieras disponibles para demostrar que el fraude ocurrió, ya que no se realizan alteraciones a los estados financieros para cubrir el delito sino que reciben pagos en efectivo “debajo de la mesa”.

La corrupción es un problema significativo para las organizaciones, particularmente en lo que se refiere al crecimiento de los mercados internacionales; a pesar de la creación de legislaciones anticorrupción en todo el mundo y de los esfuerzos realizados por las naciones y empresas para combatir este tipo de fraude, la corrupción aún representa una de las prácticas más dañinas para las organizaciones.

En la mayoría de los casos, estos crímenes son descubiertos mediante denuncias o quejas de terceras partes por medio de una línea de denuncia especializada en fraudes; por lo general, es más frecuente que la corrupción se dé en el área de compras, ya que los proveedores pueden otorgar beneficios inapropiados a los compradores de la organización, con tal de recibir preferencia por sobre otros proveedores; por tal motivo, el área de compras se considera altamente vulnerable al riesgo de corrupción. Esta última ocurre prácticamente en todos los escenarios de la vida de los mexicanos, desde los litros de 900 ml que se despachan en muchas gasolineras, hasta la liberación de personas condenadas por un delito a cambio de una retribución económica, pasando por las cuotas que los trabajadores deben entregar a sus sindicatos o el desvío de recursos del Estado con fines distintos al bienestar y el desarrollo de la sociedad (“Anatomía de la corrupción”, Organización de Mexicanos contra la Corrupción y la Impunidad).

Para más de 90% de los mexicanos, la corrupción constituye un problema y para casi 80% es un problema serio, de acuerdo con el Barómetro Global de la Corrupción 2013, elaborado por Transparencia Internacional. La Encuesta Nacional de Calidad e Impacto Gubernamental (Inegi 2015) coloca a la corrupción en segundo lugar entre los problemas más importantes para los mexicanos, con 50.9% de las menciones, sólo después de la inseguridad y antes que el desempleo y la pobreza. Algunos tipos específicos de corrupción son:

- a) **Conflicto de interés.** Ocurre cuando un empleado, gerente o ejecutivo de una organización tiene un interés económico personal no revelado en una transacción que la afecte negativamente o a los intereses de los accionistas. El conflicto de interés puede estar relacionado por lazos de parentesco, laborales o de interés personal del defraudador.
- b) **Soborno.** Consiste en ofrecer, dar, recibir o solicitar cualquier cosa de valor para influenciar un resultado, pueden ser ofrecidos a los empleados clave, así como a los administradores y a los agentes de compra que tienen discrecionalidad en la adjudicación de los negocios; por ejemplo: un agente de compras acepta sobornos para favorecer a un proveedor externo en la compra de bienes o servicios. Los sobornos ocurren en vendedores e intermediarios encargados de proveedores externos; en éstos, el defraudador “compra” influencia para procurar un beneficio que es contrario a los derechos de otros y en donde, por lo general, se encuentran dos partes coludidas.
- c) **Agradecimientos ilegales.** Este esquema ocurre cuando una persona otorga un objeto de valor a otro para afectar sus decisiones, generalmente sucede después de que se ha tomado una decisión; este tipo de regalos ilegales son similares a la corrupción; sin embargo, se diferencian en que no necesariamente intentan influenciar una decisión antes de ser tomada. Ocurre después de que un acto se ha realizado y se da en gratitud a la persona que tomó una decisión que resultó benéfica para quien después envía el regalo ilegal.
- d) **Extorsiones económicas.** Una extorsión económica es frecuentemente lo opuesto a un caso de corrupción, la extorsión es definida como la obtención de una propiedad que pertenece a otro con su consentimiento inducido por el uso real o aparente de la fuerza y el miedo. La extorsión económica se presenta cuando un empleado mediante el uso de la fuerza o del miedo exige dinero o algo a cambio de tomar cierta decisión.
- e) **Apropiación ilegal de activos.** Son aquellos esquemas de fraude, en los cuales la persona que lleva a cabo la acción de fraude realiza sustracciones de activos o utiliza tales activos u otros recursos de la compañía

para beneficio propio; implica el robo de dinero en efectivo o bienes como: suministros, inventario, equipo e información. Algunos ejemplos de esto podrían ser el desvío de fondos por medio de recibos falsos, robo de bienes y falsificación de cheques de la empresa.

A continuación se presentan datos recabados en organizaciones acerca del robo de activos, así como las pérdidas por cada tipo de fraude. Posteriormente se describe cada uno de ellos.

Ilustración 5. Esquemas de fraude de robo de activos

Categoría	Ejemplo	Casos al año	% de casos	Pérdida promedio
<i>Skimming</i>	Irregularidad anterior al registro contable	267	14.5	\$60,000
Robo de efectivo	Sustracción con posterioridad al registro	181	9.8	\$100,000
<i>Billing</i>	Fraudes con facturas falsas	479	26.0	\$128,000
Gastos falsos	Facturas reales por conceptos falsos o excedidos	278	15.1	\$33,000
Fraude con cheques	Fraude por robo o alteración de valores	274	13.4	\$131,000
Nómina	Irregularidades mediante esquemas en el proceso de nómina	157	8.5	\$72,000
Registros falsos	Registros falsos de efectivo para conciliar acciones de fraude	55	3.0	\$23,000
Efectivo en mano	Uso indebido del efectivo de la empresa	121	12.6	\$23,000
Robo de activos	Sustracción de activos que no son dinero en efectivo	156	16.3	\$90,000

Fuente: Elaborado por el autor.

a) **Fraude en inventario y otros activos.** El equipo, suministros y otros activos que no son en efectivo pueden ser robados de diversas maneras, lo anterior puede ser desde una caja de clips hasta millones en equipamiento o tecnología. Existen básicamente dos maneras en las que un empleado puede hacerse de los bienes de la organización, la primera haciendo un mal uso y la segunda robándolos.

- Por lo general, un mal uso incluye la utilización de los vehículos de la organización, los suministros, computadoras y otro equipamiento para fines diferentes para los cuales fueron adquiridos. Por ejemplo, la utilización de equipos de cómputo de la organización para fines personales, así como la realización de funciones del personal para objetivos no establecidos.
- El robo de suministros se refiere a la sustracción de materiales, suministros y otros bienes de la organización para fines personales.

b) **Apropiación de dinero en efectivo.**

- *Robo de dinero en efectivo disponible.* Es la apropiación de efectivo acumulado en una caja chica o fondo disponible bajo la responsabilidad.
- *Robo de efectivo cobrado.* La apropiación indebida de efectivo se divide a su vez en dos tipos: el *skimming* (apropiación de efectivo antes del registro en libros) y el hurto (robo posterior al registro).
 - El robo antes del registro (*skimming*). Éste se produce cuando el dinero es robado de una organización antes de que se grave en los libros y registros de la organización. Por ejemplo, un empleado acepta el pago de un cliente pero no registra la venta; también son conocidos como fraudes fuera de libros, lo que significa que el dinero es robado previo al registro contable, lo cual representa que un esquema de *skimming* no pueda abordarse directamente mediante una auditoría. Como los fondos robados nunca se registran, la organización defraudada puede saber que el dinero nunca fue recibido; por lo tanto, es difícil detectar el dinero que ha sido robado. Es una de las formas más

comunes de fraude y puede ocurrir en cualquier punto del proceso en el que el dinero en efectivo ingresa a la organización.

Por lo general, este tipo de fraude involucra al personal de ventas, cajeros y otros que reciben dinero de forma directa por parte de los clientes; adicionalmente, algunos esquemas de fraude perpetrados por empleados se llevan a cabo a partir de pagos realizados por los clientes por correo, ya que los empleados roban los cheques sacándolos del correo.

- Robo después del registro. Se da cuando los empleados de manera intencional toman dinero en efectivo o cheques sin el consentimiento de su empleador; la diferencia de este esquema de fraude con el *skimming*, es que el dinero o cheques robados ya se encuentran registrados en los libros de la organización.
- *Desembolsos fraudulentos*. En este esquema de fraude un empleado realiza una distribución de fondos de la compañía con propósitos deshonestos; ejemplos de éstos son la falsificación de cheques, el envío de facturas falsas y algunas otras situaciones similares.
- El *lapping* o manejo indebido de efectivo consiste en tomar préstamos “temporales”, que serán reembolsados al siguiente día, pero cuya ocurrencia es repetida indefinidamente (es decir, día tras día). Es considerado una apropiación indebida de activos, porque en muchas ocasiones es el inicio de un fraude mayor en el que la intención inicial del defraudador de realizar una devolución, se ve frustrada por un acontecimiento fuera de su control.
- El esquema de reembolsos falsos ocurre cuando el defraudador procesa y registra una devolución realizada por un cliente de una mercancía previamente adquirida; la transacción indica que el objeto fue regresado al inventario y el dinero fue reembolsado al cliente, sin embargo, la devolución no ocurre de esta manera, es decir, ésta es falsa; el empleado toma el efectivo, sin existir dicho bien en reposición.
- Otro esquema en esta categoría es la manipulación de cheques, en el que el defraudador prepara fraudulentamente un cheque y genera un pago para sí mismo, proporcionando información o documentación de la organización defraudada; como por ejemplo una factura o tarjeta de control de asistencias. Por lo general, el que perpetra el fraude es quien tiene control sobre los cheques y realiza la falsificación por diversos métodos; sin embargo, pueden realizarse debido a diversas causas como una falsificación en la realización del cheque, en el endoso del cheque, alteraciones en los pagos y en la autorización del cheque.
- El fraude en nómina es cuando los perpetradores producen documentos falsos para realizar un desembolso fraudulento, falsifican una tarjeta de control de asistencias o alteran los registros de la nómina. Este tipo de fraude recae en tres tipos: empleados fantasma, horas de salario falsificadas y fraude en comisiones.
- Se conocen como empleados fantasma al fraude realizado mediante el procesamiento y emisión del pago de nómina a un empleado que no se encuentra laborando en la organización. Este tipo de fraude ocurre cuando un empleado sale de la organización y su baja no es reportada al departamento de recursos humanos; asimismo, puede realizarse mediante la duplicación de un nombre en la nómina o creando un nombre ficticio.
- Las horas de salario falsificadas son un tipo de fraude en el que se reportan horas extra laboradas por empleados que en realidad no fueron realizadas y, posteriormente, son cobradas; éstas, por lo general, son bien disimuladas para parecer realistas; sin embargo, existen parámetros de lo considerado normal para horas extra que permiten detectar estas irregularidades intencionadas.
- El fraude en comisiones es aquel en el que los empleados alteran los datos relacionados con las ventas, por ejemplo, para obtener mayores pagos como comisión; asimismo, puede ocurrir en cualquier área en el que existen recompensar por el logro de ciertos objetivos o metas.

- a) **Fraude en los estados financieros.** Implica tergiversar los estados financieros, a menudo por exagerar activos e ingresos o subestimando pasivos y gastos; este tipo de fraude es típicamente perpetrado por los que dirigen y administran la organización, con el objetivo de mejorar el aspecto económico de la misma; o, por el contrario, el de hacerla parecer más débil de lo que es financieramente para obtener beneficios o evitar pagos. Los miembros de la administración pueden beneficiarse directamente desde el fraude por la venta de acciones y recibiendo bonos por desempeño, así como utilizando reportes falsos para ocultar otro fraude.

Los fraudes en los estados financieros se realizan también para ocultar otros que han sido perpetrados y que han desfavorecido los ingresos o el capital de forma importante, de tal manera que los encargados del gobierno y supervisión de la organización no se percaten de las inconsistencias.

- *Sobreestimación de activos/ingresos.*

- Diferencias en tiempo. Este esquema se refiere al registro de ingresos y gastos en los estados financieros en periodos inapropiados. Esto puede realizarse para ajustar los egresos de acuerdo con los ingresos que son deseados.
- Ingresos ficticios. Incluyen el registro de bienes, ventas y servicios que no fueron entregados o vendidos, por lo general implican la existencia de clientes falsos o ficticios, o que algún cliente existente reporta que no recibió dicho servicio o incluso que no fue solicitado. Otra técnica utilizada por los defraudadores es ponerle sobreprecio a las cantidades en las facturas, de tal manera que reflejen montos mayores a los vendidos.
- Valuación indebida de activos. Una manera de realizar fraude en los estados financieros es tergiversando la valuación de los activos de la organización, lo cual consiste en incrementar la fortaleza de los estados financieros y sus ratios. Algunos esquemas de inflación de los activos corrientes a expensas de los activos de largo plazo, en los que el efecto neto puede observarse en el ratio corriente que divide los activos corrientes entre los pasivos para evaluar la habilidad de la organización para satisfacer sus obligaciones de corto plazo.

Algunos de las valuaciones inapropiadas de activos incluyen el aumento del inventario y las cuentas por cobrar, con el objetivo de fortalecer la apariencia de la posición financiera.

- *Subestimación de activos/ingresos.*

- Fraude fiscal o evasión. Implica la presentación de informes falsos o tergiversados a la autoridad gubernamental u otras entidades regulatorias, existen diversos métodos por el que los defraudadores pueden evadir el pago de impuestos, ya sea por la presentación de los estados financieros fraudulentos, presentación de compras falsas y donaciones inexistentes. Los paraísos fiscales son empresas creadas en el extranjero, en donde las leyes son débiles y permiten a las organizaciones evadir el pago de impuestos en los países en donde realizan sus actividades.

Para las organizaciones es de gran relevancia la comprensión de los esquemas de fraude existentes, ya sea para la creación de planes, programas y controles destinados a prevenirlos y detectarlos, así como para la investigación de los mismos.

Los presentados anteriormente son solamente algunos de los esquemas o tipos de fraude sobre los cuales se tiene registro histórico o evidencia; sin embargo, los avances tecnológicos han traído consigo nuevas formas en la realización de fraudes que las organizaciones deberán considerar en la gestión de riesgos.

Nuevas formas de fraude y sus características

La amenaza global de terrorismo digital dirigido al ataque de sistemas financieros, sistemas de defensa, bases de datos y difusión de virus ha obligado a trabajar de mejor manera y con una visión globalizada en la generación y aplicación de leyes enfocadas a castigar conductas delictivas cometidas mediante la utilización de equipos de cómputo y sistemas de comunicación, ya sea como fin o como medio.

Como respuesta para tener los elementos suficientes para prevenir, perseguir y castigar las conductas antes planteadas nos encontramos con dos vertientes; los equipos de respuesta de emergencias en cómputo y las diferentes propuestas de ley alrededor del mundo. Entre las tendencias estadísticas publicadas por este tipo de organismos encontramos:

1. Vulnerabilidades de los distintos sistemas operativos.
2. Virus detectados y medidas adoptadas para combatirlos.
3. Recomendaciones de mejores prácticas aplicadas a la seguridad de la información digital.
4. Incidentes a nivel mundial.

Esto, con el objetivo de mantener una comprensión de nuevos modos de perpetrar fraudes mediante medios electrónicos que, por lo general, tienen como objetivo el robo de información, así como el de causar daño a la estructura tecnológica, los registros y las comunicaciones.

La mayoría de los ataques a la información de la organización (que en la actualidad es el principal activo de las organizaciones) se realizan por medio de códigos maliciosos, los cuales son programas diseñados para hacer que los equipos de cómputo (móviles y fijos) realicen procesos o acciones distintas a las que fueron programados originalmente, sin el consentimiento del usuario. A continuación se enlistan los objetivos de los ataques:

- a) Ataque a sistemas de archivos.
- b) Ataque a sistemas operativos.
- c) Ataque a sistemas de procesamiento.
- d) Ataque a sistemas de comunicación.
- e) Ataque a sistemas de almacenamiento.
- f) Ataque a extensiones de archivo específicas.
- g) Ataque a aplicaciones específicas.

En el año 2012 más de 550 millones de personas fueron víctimas de este tipo de delincuentes. Los costos provocados en relación con conductas delictivas mediante tecnologías de la información fueron de \$388 000 000.00 USD en el año 2013; en el mismo periodo se calculan 431 millones de víctimas, lo que representa más de un millón por día o 14 por segundo.

En relación con las tendencias de almacenar datos e información en sistemas remotos, desafortunadamente no siempre se encuentran en el territorio donde se ofrecen sus servicios; por lo que en caso de tener problemas de fuga o pérdidas de información de sus clientes, la investigación del suceso estará dependiente de la legislación en la materia del país, donde se encuentre la infraestructura de almacenamiento de la compañía que ofrece el servicio.

Cabe hacer mención que ante la cantidad de información y datos que se albergan en un solo lugar, así como de la importancia de los clientes y empresas que alquilan este tipo de servicios, se tiene como resultado que estos esquemas de almacenamiento sean el objetivo de ataque de ciber-delincuentes que, al quebrantar un solo sistema, tendrán el acceso a mucha información útil para sus objetivos delictivos cuyas posibilidades de ser investigadas para identificar y perseguir a los mismos serán muy remotas.

Nuevas metodologías para cometer delitos surgen a la par del desarrollo de aplicaciones para hacer de los dispositivos móviles objetos indispensables; podemos mencionar el robo de identidad por teléfono y el robo de identidad por mensajes de texto, constituyen los ataques más comunes que sacan provecho de los dispositivos móviles.

En lo que respecta a los ataques cuyo origen son los propios empleados de una compañía, éstos siguen siendo una causa de preocupación ante la facilidad de los empleados de tener a su alcance información confidencial; como lo demuestra el informe de tres firmas de tarjetas de crédito de Corea del Sur, donde anuncian la infección que afectó a decenas de millones de clientes. El origen de la vulnerabilidad fue un empleado que al tener acceso a la

información robó nombres, domicilios, identificaciones oficiales y detalles de las tarjetas de crédito, simplemente copiando los datos a su memoria USB.

En resumen, para la detección e investigación de fraudes realizados por medios electrónicos, es necesario contar con conocimientos especializados en tecnología y aplicaciones, así como con controles estrictos de seguridad de la información.

La manera de detectar este esquema de fraude creciente consiste en contar con herramientas de monitoreo continuo de la estructura tecnológica de los canales de comunicación, así como del software y hardware de la organización. Asimismo, se deben desarrollar técnicas y procedimientos para evaluar la vulnerabilidad de los sistemas a ataques o fraudes cibernéticos que provienen tanto del exterior como del interior de la organización.

1.3 Comprensión y análisis del fraude

1.3.1 Teoría del fraude

Los esquemas de fraude presentados anteriormente han sido identificados posterior a largos periodos de investigación, obtención de información y análisis de casos en todo tipo de organizaciones públicas y privadas en todo el mundo.

Derivado de estos estudios se han encontrado patrones de comportamiento y circunstancias que se encuentran presentes consistentemente en casos de fraude; uno de los más importantes estudiosos del fraude es Donald Cressey, quien en 1961 identificó que todos los casos de fraude estudiados tienen en común que el defraudador presenta tres factores que los predisponen y hacen de mayor riesgo la comisión del delito, a los que denominó “Triángulo del fraude” y son el motivo, presión o incentivo, la oportunidad y la racionalización.

El triángulo del fraude suele observarse en los defraudadores cuyos estándares de moralidad es alta, correspondiente a 80% de la población, ya que requieren tener un motivo que genera presión sobre ellos, así como de la oportunidad brindada por débiles controles de la organización o por la facilidad de acceder a los bienes de la misma debido a su posición y, finalmente, racionalizan el acto estableciendo una justificación moralmente aceptable desde su punto de vista. Un defraudador profesional no cuenta con estos factores, ya que el fraude es su actividad principal para obtener ingresos.

Ilustración 6. Triángulo del fraude



Fuente: Donald Cressey.

Incentivo

El primer factor del triángulo del fraude es el incentivo, mismo que ocurre cuando la administración u otros empleados tienen un estímulo o están bajo presión significativa; como por ejemplo un problema financiero o altos niveles de presión por alcanzar metas y objetivos, lo que les da una razón para cometer fraudes.

Las empresas que cotizan en bolsa son las más vulnerables a este factor, porque la presión para cumplir o sobrepasar las estimaciones de los analistas es alta; por ejemplo, es frecuente que las expectativas en ventas que tienen sea muy alta y, en caso de no ser alcanzadas, provoque que los empleados para no ser despedidos recurran a falsificar los datos en ventas o inflar las cifras reales.

Otra de las áreas de principal vulnerabilidad es la de tesorería, pues debido a la existencia de empleados con importantes necesidades financieras y presiones relacionadas con la determinación de objetivos de difícil cumplimiento, así como de un clima hostil dentro del ambiente laboral o tratos inadecuados, pueden detonar en la realización de este tipo de actividad ilegal. En esta área deberá evaluarse la existencia de las siguientes debilidades, a fin de evitar el fraude:

- Inexistencia de procedimientos tendientes a verificar el estado financiero de funcionarios claves de la compañía.
- Inexistencia de canales de comunicación adecuados para informar situaciones especiales.

Oportunidad

El factor oportunidad de un fraude se refiere a las debilidades de la organización en cuanto al control; por ejemplo: ausencia de controles, controles ineficaces y la capacidad que tiene la administración para evaluar los controles que facilitan la oportunidad de perpetrar un fraude.

En las organizaciones es cada vez más frecuente que las oportunidades de cometer fraude estén relacionadas con la falla en los controles de tecnología o el desconocimiento de los mismos; con frecuencia ocurre cuando una persona tiene acceso a información confidencial o puede realizar cambios en el software que controla información financiera. Por lo que para la prevención del fraude es de principal relevancia el control interno y la tecnología eficiente.

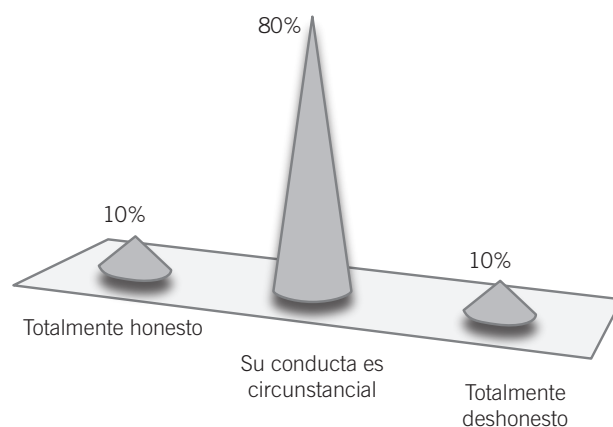
Racionalización

Es el factor de fraude que se relaciona con la moral del perpetrador, al existir una presión significativa, así como la oportunidad debido a fallas en los controles o posición del defraudador; éste normalmente encontrará una justificación al delito que comete, permitiéndole seguir con cierta estabilidad en sus labores.

La persona que racionaliza un delito o falta cometida es capaz de ajustar sus acciones con una justificación que le conceda estar en total congruencia con su código de ética personal y mantener una actitud, carácter y conjunto de valores que les permiten, consciente e intencionalmente, cometer un acto deshonesto. De acuerdo con estudios realizados por la Asociación de Examinadores de Fraude, 10% de las personas son completamente éticas, otro 10% son capaces de realizar un fraude y 80% actúan de acuerdo con la situación.

Estos datos nos muestran que 80% de los que cometen fraudes son propensos a racionalizar, porque buscan ajustar su conducta a su conciencia ética. Las principales racionalizaciones son, por ejemplo: “He trabajado mucho sin recompensa, por lo que merezco obtener más dinero a cambio”, “Todo el mundo lo hace”, “Será un préstamo temporal”, entre los más comunes.

La gerencia puede disminuir la racionalización para la comisión de un fraude por medio de acciones de implementación de prácticas remunerativas y de trabajo justas, así como fortaleciendo el tono en la cima que es el ejemplo a seguir que la gerencia da con referencia al respeto por los controles establecidos y teniendo una filosofía de gestión que promueva la ética y el buen funcionamiento de los recursos humanos en la organización.

Ilustración 7. Probabilidad de conducta ilícita o deshonesta

Fuente: ACFE.

La comprensión del triángulo del fraude permite el diseño de planes de prevención de fraude de manera efectiva, considerando los riesgos en cada uno de los colaboradores de la organización, así como los riesgos relacionados con el tipo de actividad y posibles esquemas de fraudes perpetrados.

Existen dos enfoques mediante los cuales pueden implementarse medidas para mitigar los efectos de los tres elementos:

Enfoque 1: Racionalización-Presión (Control)	Enfoque 2: Oportunidad (Sustantivo)
Código de ética	Software con parámetros de control y sistema de alerta de irregularidades detectadas
Manuales de conducta	Aplicación de Ley Bendford
Política de Recursos Humanos	Modelos analíticos automatizados
Evaluación del clima laboral	Uso de análisis de fraude predeterminados en análisis de circuitos
Línea de reporte de irregularidades	Minería de datos

Investigaciones recientes añaden una nueva variable que influye en el fraude, ésta es la capacidad, y con esto el “Triángulo del Fraude” se sustituye por el “Diamante del fraude”. En este modelo se incorpora la capacidad del individuo para cometer el fraude, debido a que estadísticamente aquellos fraudes cuyo impacto ha sido mayor en la organización han sido cometidos por personal de alto perfil; por tal motivo, es necesario considerar tanto las características personales como el nivel de habilidades de los mismos.

Ilustración 8. Diamante del fraude

Fuente: ACFE.

Es importante considerar la variable “capacidad”, porque los sistemas de control y detección de la organización deberán estar preparados para detectar defraudadores de todo tipo; desde personas comunes que debido a presiones excepcionales realizan un acto de fraude y hasta aquellos que cuentan con capacidades e incluso redes de delincuencia organizada y que pueden infringir grave daño a la organización.

El sistema de control deberá tener en cuenta algunas señales de alerta que se han obtenido después de años de estudio de los casos que han existido; estas señales de alerta o banderas rojas son solamente indicios y existen en el mercado herramientas informáticas que permiten un monitoreo continuo de los mismos por medio de la base de datos y redes de comunicación de la organización.

1.3.2 Indicadores de la ocurrencia de fraude (banderas rojas)

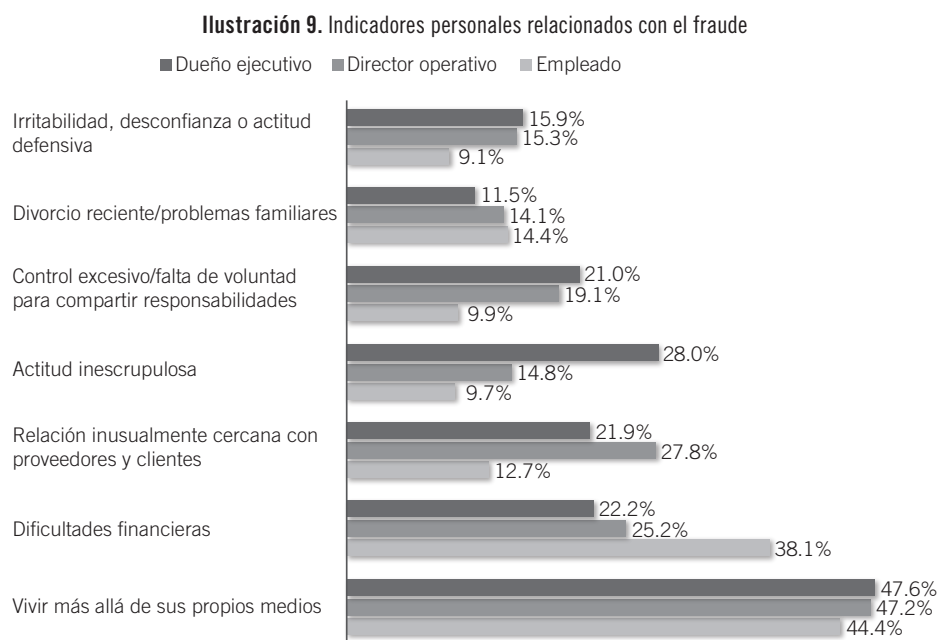
Por medio de la experiencia de diversas organizaciones donde ha ocurrido un fraude corporativo y también de investigaciones de organismos internacionales se han logrado determinar ciertos indicadores que frecuentemente señalan la existencia de un fraude. Es de gran relevancia que los miembros de la organización, la gerencia, auditores internos y externos, organismos reguladores y otras partes interesadas, puedan detectar estas alertas y conozcan el procedimiento a seguir a partir de la detección.

Los indicadores de fraude pueden ser de diversa naturaleza, por lo que deben entenderse en su conjunto y utilizarse técnicas apropiadas para su investigación, algunos ejemplos son:

- a) **Indicadores personales.** Son aquellas señales de alertas que pueden ser comportamientos inusuales como: actos ilegales, estilos de vida costosos, vacaciones no tomadas, personal de baja calidad, empleados trabajando fuera del horario laboral, remuneración ligada a los resultados financieros, origen dudoso de las utilidades, segmentos de negocio conocidos por pocos empleados y personas autoritarias que evaden los controles.

Estos indicadores se relacionan más bien con comportamientos inusuales como: estrés excesivo, comportamiento irritable o sospechoso, que no son congruentes con la conducta del empleado o colaborador a lo largo del tiempo y por lo que la gerencia o las áreas encargadas de supervisión deberán detectar de inmediato para verificar que no estén ocurriendo acciones indebidas.

De acuerdo con el Reporte a las naciones publicado por la ACFE en 2016, las principales conductas observadas como banderas rojas y que se relacionan con el puesto de quien comete el fraude se muestran a continuación:



Fuente: Reporte a las naciones, ACFE, 2016.

- b) **Comerciales y financieros.** Las banderas rojas relacionadas con los ratios financieros son indicadores que demuestran inconsistencias en los datos, al compararlos unos con otros y los resultados obtenidos no coinciden con los esperados. Un ejemplo sería comparar el volumen de ventas con los ingresos financieros del mes, mismos que deberían aumentar de manera proporcional y, en caso de no ser así, esto sería un indicador de ocurrencia de fraude o alguna irregularidad.

Otros tipos de indicadores en esta categoría se relacionan con: una baja moral, alta rotación de los directivos, poco seguimiento y control sobre las metas, crecimiento de las ventas, niveles anormales de rentabilidad que pueden indicar la existencia de transacciones fuera de lo convencional, una estructura de sistemas insuficiente para el volumen y naturaleza de las operaciones de una compañía, utilidades por encima del promedio de la industria, desajuste entre el crecimiento y el desarrollo de los sistemas, reputación pobre, problemas de liquidez, estructuras complejas y el uso de organizaciones “paralelas”.

- c) **Indicadores estructurales.** Es importante indagar y registrar los sitios remotos mal supervisados, la búsqueda de resultados a cualquier costo, origen de ingresos sin relación con objeto social, negocios que son complejos de entender y donde la comunicación entre firmas es mínima; la administración puede envolverse en un nivel tan extremo con el logro de metas financieras u operativas que esto se convierte en un blanco dominante a expensas de la productividad o eficiencia a largo plazo.

Las banderas rojas varían de acuerdo con la industria, las cuentas contables y los ciclos de negocios, debido a que existen áreas especialmente propensas a manipulación o robo. A continuación se analizan algunas cuentas específicas de alto riesgo incluyendo indicadores de fraude, que si bien el conocerlas nos ayuda a prevenir el fraude con mayor eficacia, no asegura su detección. Sin embargo, el conocimiento de estas señales y de las técnicas de detección de fraude aumenta la posibilidad del auditor de identificar errores a consecuencia del fraude.

Riesgo de fraude en ingresos y cuentas por cobrar

Un estudio realizado por COSO descubrió que más de la mitad de los fraudes en los estados financieros implicaban ingresos y cuentas por cobrar; esto se debe a que estas cuentas y las de efectivo son particularmente susceptibles a la manipulación y robo. De igual manera las ventas, que con frecuencia son realizadas en efectivo o se convierten con rapidez en efectivo, por lo cual son altamente vulnerables. Algunas señales de advertencia de fraude en estas cuentas son:

- a) Ingresos ficticios.
- b) Reconocimiento anticipado de ingresos.
- c) Manipulación de ajustes para los ingresos.
- d) Señales de advertencia del fraude de ingresos.
- e) Discrepancias documentales.
- f) Malversación de entradas que involucran al ingreso.
- g) Falla para registrar una venta.
- h) Robo de entradas de efectivo después de que se registra una venta.
- i) Señales de advertencia de malversación de ingresos y entradas de efectivo.

Riesgo de fraude en inventario

El inventario con frecuencia es la cuenta más importante en el saldo de varias empresas y a veces es difícil verificar y realizar una valuación de las existencias; como resultado, el inventario es susceptible a manipulación para el logro de fines de los informes financieros, así como vulnerable de ser vendido o malversado. Algunas de las señales de alerta en el inventario son:

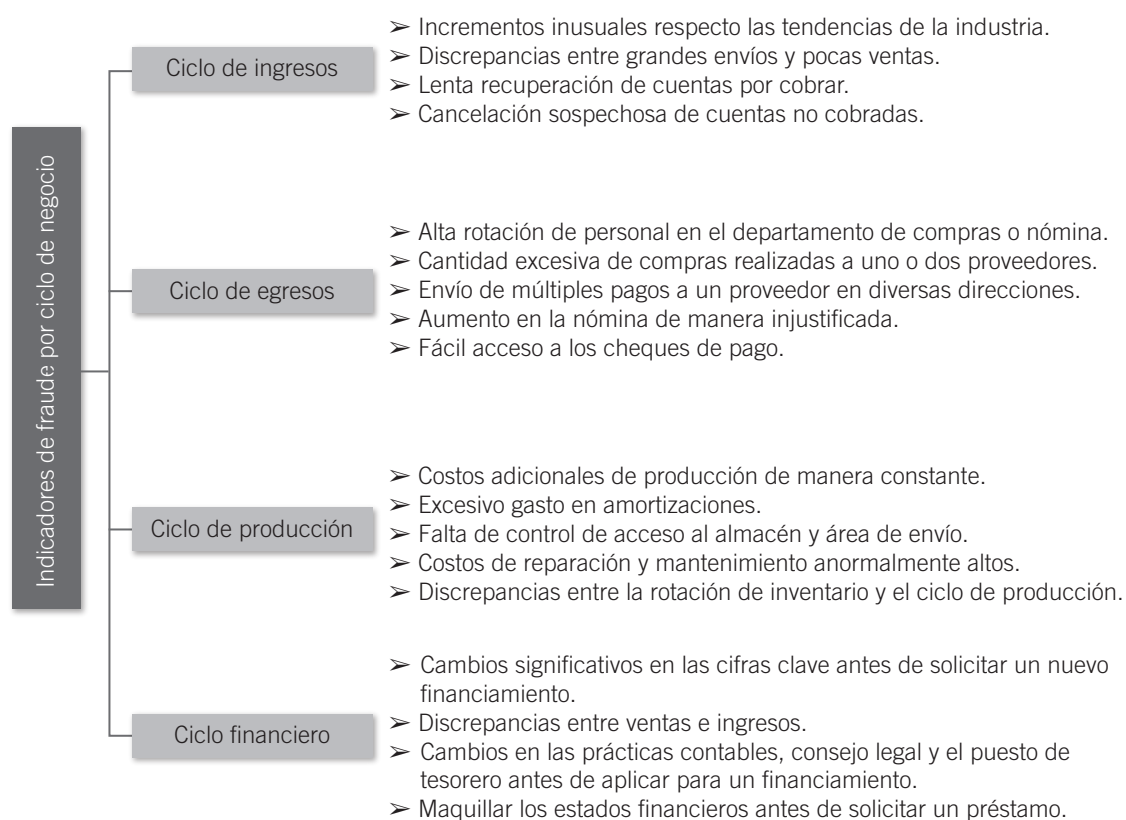
- a) Inconsistencia en los registros contra las existencias.
- b) Personal de almacén mantiene una relación cercana con los de recepción de mercancías y ventas.
- c) No se realizan revisiones de inventario.
- d) Falta de correlación de la producción con las existencias y las ventas.

Riesgos de fraude de compras y cuentas por pagar

Los casos de informes financieros fraudulentos que involucran cuentas por pagar son relativamente comunes, aunque menos frecuentes que los fraudes que involucran inventarios y cuentas por cobrar; la subestimación deliberada de las cuentas por pagar, por lo general, ocasiona la subestimación de las compras y costos de productos vendidos y una sobrestimación del ingreso neto. Las malversaciones importantes que involucran compras también pueden ocurrir en la forma de pagos a proveedores ficticios, al igual que el pago por parte de empleados y otros arreglos ilegales con los proveedores.

A continuación se presentan algunas de las banderas rojas más comunes por ciclo de negocios:

Ilustración 10. Indicadores de fraude por ciclo de negocio



Fuente: Elaborado por el autor.

1.3.3 Perfil del defraudador

Por medio de diversas investigaciones podemos, a partir de los indicadores y casos de fraude en organizaciones del mundo, definir algunas de las características que comúnmente presentan los perpetradores de fraude. De acuerdo con estudios y estadísticas se ha identificado el perfil más frecuente de defraudador, quien es generalmente un hombre de edad media que ha sido empleado durante varios años en la empresa; trabaja en el departamento financiero y realiza el fraude en sus propios términos. La mayoría de las ocasiones impulsado por el deseo de dinero y

la oportunidad, con frecuencia también forma parte de la gerencia y, en muchas ocasiones, ocupa un puesto de confianza al tener un nivel educativo alto, con familia y puede pertenecer a organizaciones comunitarias.

Nivel de autoridad

Es menor la cantidad de fraudes cometidos por ejecutivos de alto nivel en las organizaciones; sin embargo, éstos son los que provocan pérdidas mayores; lo anterior debido a que personas de este perfil suelen tener mayor acceso a los activos de la organización que los empleados de niveles menores, así como una mayor capacidad de eludir controles clave.

Antigüedad en la organización

Las personas que han pasado más tiempo en la organización, si cometieran un fraude generarían un impacto económico mayor, debido a que con frecuencia ocupan puestos de autoridad y conocen el entorno operativo porque cuentan con mayores capacidades y relaciones en el negocio.

Área laboral

Las áreas laborales más vulnerables al fraude según ACFE son: contabilidad (16.6%), operaciones (14.9%), ventas (12.4%) y alta dirección (10.9%). Se ha encontrado que el área encargada de las finanzas y de la contabilidad tiene una mayor probabilidad de cometer fraudes, por lo que se debe intensificar la supervisión y controles en la misma. De igual manera, los fraudes en la alta dirección son aquellos con una frecuencia más baja de ocurrencia, pero que ocasionan las mayores pérdidas financieras; por lo anterior, la duración que puede tener el fraude y los montos defraudados sin tomar en cuenta la pérdida de reputación de la organización también es de menor tiempo.

Género

De acuerdo con las estadísticas publicadas, 69% de los defraudadores son hombres y 31% mujeres, lo anterior porque la estructura de la fuerza laboral está constituida por hombres y son ellos quienes ocupan puestos de mayor responsabilidad actualmente.

Edad

Cincuenta y cinco por ciento de los defraudadores tiene entre 31 y 45 años al cometer el fraude; sin embargo, a mayor edad del defraudador la frecuencia de fraude es menor, pero el impacto económico que ocasionan es mucho mayor; por tal motivo, el comportamiento e indicadores de inestabilidad en este grupo de edad debe ser observado.

Nivel académico

Los defraudadores tienen títulos universitarios y ocupan puestos de autoridad; se ha encontrado la correlación de que a mayor grado académico del defraudador, el impacto económico del fraude tiende a ser mayor porque involucra mayor inteligencia en su planeación y ejecución.

Éstos son algunos de los indicadores relacionados con el perfil del defraudador que deberán ser tomados en cuenta al elaborar planes para prevenir y detectar fraudes; sin embargo, no excluyen la existencia de perfiles atípicos, por lo que la mayor recomendación es realizar un monitoreo continuo de personal que presentan indicadores de riesgo.

1.4 El fraude en las organizaciones y el impacto de la auditoría forense

Ante los esquemas de fraude cada vez más avanzados y del conocimiento obtenido a partir de casos examinados, las organizaciones deben tomar medidas que les permitan controlar este aspecto en sus organizaciones; en donde la mejor estrategia es la prevención de conductas fraudulentas que impactan gravemente a la organización en sus finanzas, reputación y estructura interna.

La prevención del fraude implica la implementación de políticas y procedimientos, la capacitación de los empleados y la comunicación de la gestión para educar a los empleados sobre las actividades fraudulentas. De igual manera, la detección del fraude implica actividades y programas diseñados para identificar el fraude y la mala conducta que está ocurriendo o ha ocurrido.

La disuasión del fraude consiste en inducir a alguien con razones a desistir de un propósito; disuadir también se basa en la identificación del objetivo y en eliminar las acciones para realizarlo.

Existen diversos autores y organizaciones que sugieren los elementos con los que deberá contar un buen sistema de prevención y detección de fraude, que contemple de manera orgánica los factores de riesgo más importantes para la organización.

Por ejemplo, el AICPA (Instituto de Contadores Públicos certificados de EE.UU.), en conjunto con varias organizaciones profesionales, ha publicado la “Guía para ayudar a prevenir, disuadir y detectar fraudes para apoyar a la administración y consejo directivo en sus esfuerzos contra el fraude”. Esta guía identifica tres acciones para prevenir, disuadir y detectar fraudes:

1. Crear y mantener una cultura de honestidad y altos estándares éticos.

- Determinación de los estándares desde los niveles altos de la administración.
- Creación de un ambiente de trabajo positivo.
- Contratación y promoción de los empleados adecuados.
- Entrenamiento de todos y especialmente nuevos empleados.
- Confirmación de que los empleados confirmen de manera periódica sus responsabilidades, con el fin de cumplir con el código de conducta.
- Disciplina, es decir, que los empleados deben saber que pueden ser responsabilizados por no seguir el código de conducta de la compañía.

2. Evaluar los riesgos de fraude y aplicar programas y controles para mitigar los riesgos de fraude identificados.

El fraude no puede ocurrir sin la percepción de la existencia de una oportunidad para cometer y lograr el acto; la administración es responsable de identificar y medir los riesgos de fraude, de implementar acciones para mitigar los riesgos identificados y de monitorear los controles internos que impiden y detectan el fraude.

3. Desarrollar un proceso adecuado de vigilancia de fraude.

El comité de auditoría tiene la responsabilidad fundamental de vigilar los informes financieros de la organización y los procesos de control interno, al realizar esta función el comité de auditoría debe considerar la posibilidad de que la administración pase por encima de los controles internos y vigila su proceso de evaluación de riesgo de fraude; al igual que sus programas y controles contra el fraude.

El comité de auditoría también apoya la creación de altos estándares efectivos relacionados con la importancia de la honestidad y el comportamiento ético al reforzar la cero tolerancia al fraude de la administración. La vigilancia del comité de auditoría sirve para disuadir a los altos niveles de la administración de la comisión de algún fraude.

La mayor parte de los estatutos del comité de auditoría le autorizan a investigar cualquier asunto dentro del ámbito de sus responsabilidades de vigilancia, por lo general, tienen la autoridad para utilizar los servicios de asesores legales, de contabilidad y otros profesionales expertos en fraudes para apoyar en cualquier investigación de fraude.

Debido a que el comité de auditoría tiene una función importante en la determinación de estándares morales altos adecuados al vigilar las acciones de la administración; el estándar 2 del PCAOB (Public Company Accounting Oversight Board-Junta de Supervisión de Contabilidad de las Empresas Públicas) requiere que los auditores de compañías cuyas acciones se comercializan en el mercado de valores, evalúen la efectividad del comité de

auditoría como parte de la evaluación del auditor de la efectividad de la operación de controles internos sobre los informes financieros.

Normalmente se obtienen buenos resultados cuando interactúan el comité de auditoría, la auditoría interna y el auditor externo; este estándar indica que la vigilancia ineficaz por parte del comité de auditoría es, por lo menos, una deficiencia importante y puede ser un fuerte indicador de una debilidad material en el control interno sobre los informes financieros. De acuerdo con las mejores prácticas internacionales se ampliarán los siguientes elementos básicos de un efectivo sistema para prevenir y detectar fraudes:

1. Sistema de evaluación de riesgos de fraude y de establecimiento de controles.
2. Estructura de roles y responsabilidades del personal y las áreas para la prevención y detección de fraudes.
3. Medios de comunicación directa con la alta dirección y el consejo de administración para la denuncia de fraudes e indicios.
4. Política de ética organizacional y antifraude, así como métodos que mantengan un clima ético en la organización.

1.4.1 Evaluación de riesgos de fraude y establecimiento de controles

1.4.1.1 Evaluación de riesgos y controles corporativos

El sistema de evaluación de riesgos y controles de fraude dentro de la organización se encuentra inmerso en un sistema de gestión de riesgos corporativo, el cual es más general e incluye los riesgos que son prioritarios para la organización; en este sistema corporativo participan todos los miembros de la organización con distintos niveles de responsabilidad, en el que los principales responsables son el consejo de administración y la alta dirección. Derivado de la evaluación de riesgos se realiza una evaluación e implementación de controles, lo que permite que los riesgos encontrados sean mitigados al considerar el control interno como un proceso efectuado por la dirección de una entidad, la administración y otros miembros de la empresa; el cual es diseñado para proporcionar un grado de seguridad razonable referente a los siguientes objetivos:

- Cumplimiento de eficacia y eficiencia.
- Generación de información confiable.
- Cumplimiento de leyes y regulaciones.

Específicamente la organización puede lograrlo mediante:

- La identificación del universo de controles existentes y la cuantificación de los costos asociados con la operación y validación de dichos controles.
- La identificación de los controles que mitiguen y manejen los riesgos de la manera más eficaz y eficiente buscando obtener el mejor nivel de control posible.
- Rediseño, automatización o implementación de nuevos controles que permitan incrementar la eficiencia y eficacia del sistema de controles existentes.
- El diseño e implementación de una supervisión mediante los altos ejecutivos y una estructura de reporte para monitorear la efectividad del sistema de control, su infraestructura y la identificación de mejoras del proceso.

Para la planeación e implementación de este sistema existen diversos marcos que sirven como estructura guía para mantener un control efectivo de los riesgos, dar respuestas a éstos y lograr los objetivos de la organización. El más utilizado a nivel internacional por organizaciones tanto del sector público como privado es el marco COSO, diseñado por la comisión de organizaciones patrocinadoras *Treadway (Sponsoring Organizations of the Treadway Commission)*, a raíz de diversos escándalos internacionales relacionados con el fraude en estados financieros. Este marco considera que toda organización tiene tres tipos de objetivos (informe, operaciones y cumplimiento), que

deberá alcanzar por medio de la aplicación de medidas de control en cinco componentes identificados: entorno de control, evaluación de riesgos, actividad de control, información y comunicación y monitoreo.

Ilustración 11. Marco Integrado de Control COSO

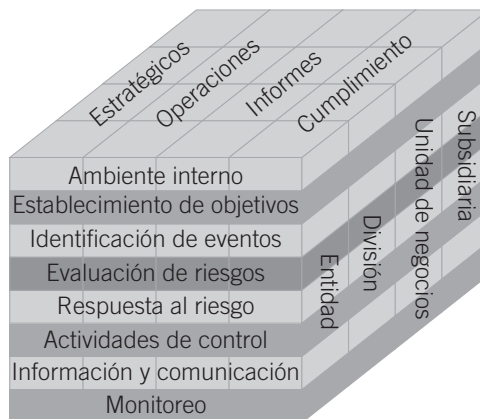


Fuente: COSO.

En 2013 COSO publica una actualización denominada COSO-ERM, este marco es más amplio que la versión anterior porque se enfoca en la identificación, evaluación y control de los riesgos añadiendo componentes al cubo. Asimismo, incluye los objetivos estratégicos como primordiales para contemplar en la gestión de riesgos organizacionales; la correcta implementación de este marco da cumplimiento a los requerimientos de la Ley Sarbanes-Oxley de Estados Unidos de América.

COSO-ERM define la gestión de riesgo empresarial como un proceso que efectúa el consejo directivo, la dirección y otro personal de una entidad, mismo que se aplica al establecimiento de estrategias y se concibe para identificar los eventos potenciales que pueden afectar a la entidad. De igual manera se emplea para gestionar los riesgos que se encontrarán dentro del apetito de riesgos, con la finalidad de proporcionar un aseguramiento razonable respecto del logro de los objetivos de la entidad.

Ilustración 12. Marco Integrado de Gestión de Riesgos Empresariales COSO-ERM



Fuente: COSO.

Los marcos de control COSO y COSO-ERM no son los únicos que sirven de referencia para la implementación de un sistema de gestión de riesgos y controles efectivo; los marcos utilizados pueden variar de un país a otro debido a la legislación o a preferencias de las organizaciones. COSO es el más utilizado en comparación con otros marcos de control que se presentan a continuación y en donde se comparan sus características.

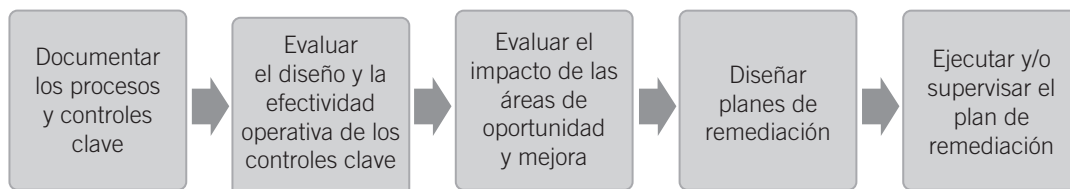
Ilustración 13. Cuadro comparativo de marcos de control

Características	COSO	COSO-ERM	COBIT	CoCo	King	MECI
Enfoque o prioridad	Control interno	Gestión de riesgos	Auditoría de TI	Auditoría interna	Gobierno corporativo	Control interno en el sector público
Definición	Es un proceso efectuado por el consejo, la alta dirección y otro personal, diseñado para proveer aseguramiento razonable respecto al logro de los objetivos.	La gestión de riesgos es un proceso efectuado por el consejo, la alta dirección y otro personal, enfocado en el logro de la estrategia en toda la organización, diseñado para identificar eventos potenciales que pueden afectar a la organización y gestionar el riesgo de acuerdo con el apetito de riesgo, para proveer aseguramiento razonable respecto al logro de los objetivos.	El objetivo de los controles de tecnología es la creación de valor para las partes interesadas mediante la creación de beneficios, optimización de riesgos y uso óptimo de recursos.	Son acciones que se enfocan en obtener los mejores resultados de la organización. Incluye recursos, sistemas, procedimientos, cultura, estructura y tareas.	Enfatiza el liderazgo con una base ética y la necesidad de rediseñar la organización alrededor de la sustentabilidad (que es la suma de la innovación, justicia y colaboración).	Proporciona la estructura básica para evaluar la estrategia, la gestión y los propios mecanismos de evaluación del proceso administrativo, aunque promueve una estructura uniforme.
Componentes/Principios	- Ambiente de control - Evaluación de riesgos - Actividades de control - Información y comunicación - Monitoreo	- Ambiente de control - Fijación de objetivos - Identificación de eventos - Evaluación de riesgo - Respuesta al riesgo - Actividades de control - Información y comunicación - Monitoreo	- Cumplir con las necesidades de las partes interesadas - Cubrir la empresa de extremo a extremo - Aplicar un solo marco integrado - Enfoque holístico - Separar la gobernanza de la gerencia	- Propósito - Compromiso - Capacidad - Seguimiento y aprendizaje	- Disciplina - Transparencia - Independencia - Rendición de cuentas - Responsabilidad - Justicia - Responsabilidad social	- Autocontrol - Autogestión - Autorregulación

Fuente: Elaborado por el autor.

Método para evaluar los riesgos y controles internos bajo el marco COSO

Ilustración 14. Proceso para evaluar riesgos y controles bajo el marco COSO



Fuente: COSO.

Este proceso para evaluar el marco de COSO consta de cinco fases:

1. **Documentar procesos y controles clave.** Esta fase consiste en documentar y clarificar procesos que son de gran relevancia, los cuales deben estar identificados y documentados, para ello pueden utilizarse las siguientes herramientas:

- a) *Diagrama de flujo.* El objetivo de un diagrama es proveer una descripción gráfica de la naturaleza, flujo, componentes y camino crítico de un proceso; utilizando símbolos gráficos y palabras.
- b) *Narrativas.* Éstas representan la descripción detallada de las actividades realizadas como parte del proceso, por lo cual se recomienda seguir una estructura lógica similar al diagrama de flujo con el objeto de vincular ambos documentos.

Asimismo, las narrativas deberán contener suficiente información para facilitar el entendimiento del flujo de las actividades y/o transacciones relacionadas con las cuentas significativas de los estados financieros.

- c) *Matriz de funciones y responsabilidades.* Identifican, de manera resumida, las actividades asignadas a cada posición o puesto dentro de la organización, con el objeto de identificar cualquier incompatibilidad de funciones asignadas (segregación de funciones).
- d) *Elaboración de matriz de riesgos y controles.* La matriz de riesgos y controles permite evaluar si los controles están adecuadamente diseñados para mitigar los riesgos e identificar los controles clave.

Los atributos de los controles se deben identificar como:

- Si se tratara de controles preventivos o detectivos.
- Si fueran controles manuales o automatizados.
- Si se tratara de controles clave, aplicativos o de monitoreo, redundantes o compensatorios.
- Si se tratara de controles aplicados a nivel corporativo.
- Periodicidad.

Con el objeto de construir un escenario integral es necesario especificar los siguientes elementos en la documentación que se elabore:

- Las aplicaciones informáticas que soportan el proceso.
- La descripción detallada de las actividades de control, identificando los elementos básicos de dichos controles, por ejemplo: quien ejecuta la actividad de control, cómo la realiza, con qué, para qué y con qué periodicidad.

Los controles deben describir lo siguiente:

- ¿Quién lo hace?
- ¿Qué hace?
- ¿Por qué este control se ejecuta?
- ¿Cuándo se ejecuta?
- ¿Cómo se completa?
- ¿Cuáles son las salidas de los controles?

e) *Identificación de los reportes, formatos o archivos que se generan.*

2. **Evaluar el diseño y efectividad operativa de los controles clave.** Para evaluar el diseño y efectividad de los controles deberá diseñarse un plan de pruebas, que deberán establecer los siguientes elementos para la ejecución de las mismas:

- a) Establecer si las pruebas serán realizadas de manera manual o con apoyo de aplicaciones informáticas.
- b) El periodo en que las pruebas serán ejecutadas.
- c) Técnicas de evaluación.
- d) Tamaño de la muestra.
- e) Definir los criterios de evaluación.

Una de las pruebas más comunes para verificar los controles documentados es la ejecución de los denominados recorridos de procesos, los cuales tienen el fin de verificar si los procesos documentados son congruentes con la ejecución real de los controles; asimismo, tiene dos enfoques, primero confirmar el entendimiento del proceso y, segundo, evaluar de manera simultánea la efectividad del diseño de los controles establecidos. El recorrido permitirá confirmar que:

- a) El diagrama de flujo representa la forma en que la compañía opera.
- b) Los controles existen y funcionan como fueron diseñados.
- c) La segregación de funciones documentada es la que realmente opera.
- d) Los reportes son generados como producto del proceso.

3. **Evaluar el impacto de las áreas de oportunidad y mejora.** Finalmente, deberá emitirse un informe en el que deberán detallarse las áreas de oportunidad y mejora, identificadas con motivo de las pruebas de control, así como el reporte deberá indicar la causa raíz y el impacto de cada deficiencia. El impacto de las deficiencias encontradas se relaciona con las pérdidas esperadas debido a la falla o inexistencia de un control clave y se calcula por la probabilidad e impacto de ocurrencia.

4. **Diseñar planes de remediación.** El plan de remediación deberá describir las actividades que deberán ser realizadas para subsanar las deficiencias identificadas, y como resultado se podrá construir un cronograma para llevar a cabo las actividades de remediación; ponderando el impacto y el nivel de esfuerzo requerido para corregir las deficiencias y, a la vez, indicando a la persona responsable de llevar a cabo dichas actividades de remediación y el tiempo definido para su ejecución.

5. **Ejecutar y supervisar el plan de remediación.** Los planes y medidas sugeridas deberán ser supervisados por las personas designadas, ya que en caso de no ser implementadas de inmediato, pueden causar pérdidas o la materialización de los riesgos identificados.

Sistema de evaluación de riesgos de fraude

Bajo el esquema general de la evaluación de riesgos y controles se encuentra la evaluación del riesgo de fraude, la cual es la probabilidad de que éste se produzca y las posibles consecuencias para la organización. La probabilidad de que ocurra una actividad fraudulenta se basa, por lo general, en cuán difícil sería cometer el fraude, en los factores de motivación que llevarían a este último y los antecedentes históricos que la organización posea en cuanto al mismo.

Con frecuencia, la evaluación de riesgo de fraude constituye un componente crítico de un programa más grande de gestión de riesgos corporativos, constituye una herramienta útil para la gerencia y los auditores internos, que les permite identificar sistémicamente dónde y cómo puede perpetrarse un fraude, así como quiénes pudieran estar en posición de cometerlo.

Una revisión de los riesgos a los que una empresa se ve expuesta, representa un paso esencial para aliviar las preocupaciones que el consejo y la alta dirección tienen con respecto a los riesgos de fraude, así como su capacidad para alcanzar las metas organizacionales mientras se promueve la confianza pública en la salud de una organización. Una evaluación de riesgo de fraude se concentra en esquemas y escenarios de fraude para determinar la presencia de controles internos y si éstos pueden ser eludidos.

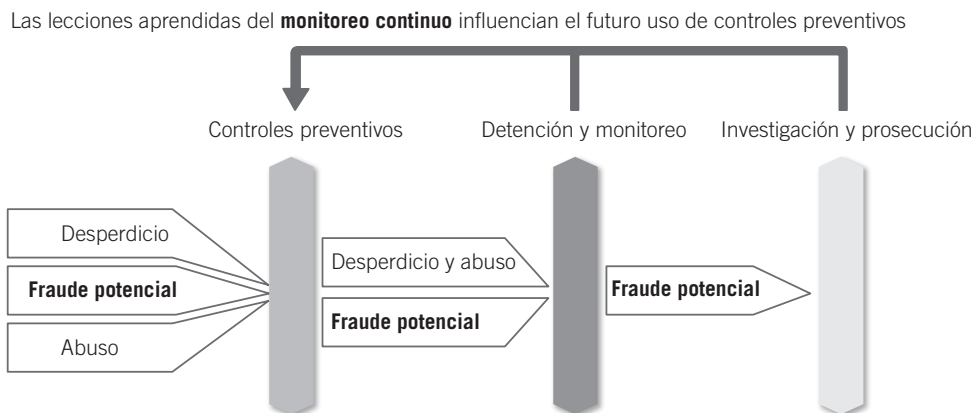
Una importante función de la gerencia es la de proporcionar vigilancia para el cumplimiento exitoso de una evaluación de riesgo de fraude; de manera que la gerencia adquiera mayor y mejor comprensión de los riesgos y de los controles que se encuentran implantados para mitigar tales riesgos. El alcance de la evaluación de riesgo de fraude podría variar ampliamente, dependiendo del tamaño de la organización, su complejidad o el tipo de industria a la que pertenece; por ejemplo, un negocio en línea que cuente con pocos empleados, con existencias limitadas de inventarios y escaso dinero en efectivo, tendría probablemente distintos riesgos de fraude comparados con los que tendría una organización que posea numerosas ubicaciones físicas y una importante cantidad de empleados con acceso a las existencias de inventarios y al dinero en efectivo.

De acuerdo con el marco COSO y aplicando los componentes al riesgo específico de fraude, la evaluación e implementación de controles antifraude se comprende de la siguiente forma:

1. **Entorno de control.** Elementos con un fuerte entorno de control ayudan a prevenir el fraude, incluyendo un código de conducta, políticas éticas y políticas de fraude para establecer el marco adecuado en la alta dirección. Un código de ética y programas de una línea directa de denuncias son útiles en la prevención del fraude, así como la contratación y promoción de las directrices, las prácticas de supervisión por el comité de auditoría y la junta directiva.
2. **Evaluación de riesgos.** Es el establecimiento de procesos para evaluar riesgos de fraude que tenga en cuenta los factores y esquemas de fraude; mismos que deberán realizarse de forma regular y en los que se deberá asegurarse la participación apropiada del personal encargado de ejecutar los procesos.
3. **Actividades de control.** Son las políticas y procedimientos para los procesos de negocios, incluidos los límites de autoridad apropiada y segregación de funciones incompatibles.
4. **Información y comunicación.** Es la promoción de la importancia del programa de gestión del riesgo de fraude y la posición de la organización sobre el mismo, tanto interna como externamente por medio de programas de comunicación corporativa; también pueden considerarse el diseño y capacitación para concientizar al personal acerca del fraude. Confirmar si los empleados conocen las políticas establecidas y si las están cumpliendo de una manera adecuada.
5. **Monitoreo.** Proporcionar una evaluación periódica de controles antifraude, el uso de las evaluaciones independientes del programa de gestión del riesgo de fraude por auditoría interna u otros grupos; de igual manera, la implementación de la tecnología para ayudar al continuo monitoreo.

De esta forma y de acuerdo con el marco COSO, el riesgo de fraude se gestionaría como muestra la siguiente gráfica:

Ilustración 15. Marco integrado de control interno aplicado al fraude

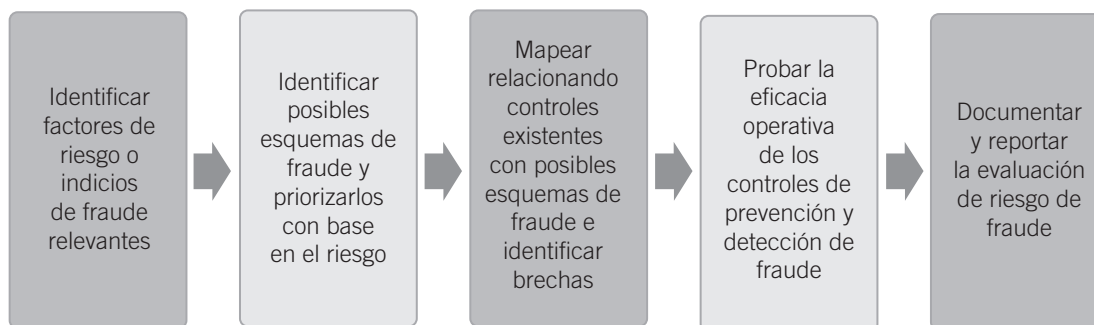


Fuente: Instituto de Auditores Internos, 2016.

Los métodos de detección de fraude deben ser flexibles, adaptables y continuamente renovados para satisfacer los cambios en el entorno de riesgo; mientras que las medidas preventivas son de fácil identificación.

Con base en la comprensión de lo anterior concluimos que el riesgo de fraude es uno de los más importantes que la organización debe gestionar mediante un proceso sistemático. A continuación se presenta un procedimiento para realizar dicha evaluación por medio de cinco fases propuestas por el Instituto de Auditores Internos.

Ilustración 16. Proceso para gestionar el riesgo de fraude



Fuente: Instituto de Auditores Internos, 2016.

Identificar factores de riesgo de fraude relevantes

El primer paso es el de recolectar información sobre las actividades de negocio de la organización, con el fin de lograr una comprensión de los riesgos de fraude asociados; la información a recopilarse debe considerar también datos de los socios.

Este proceso incluye una revisión de la documentación de fraudes previos y fraudes sospechados cometidos en contra de o en nombre de la organización; evaluación de fraudes relacionados con organizaciones similares y revisión de las medidas de desempeño adoptadas por la organización en el transcurso de los últimos años en comparación con la competencia. Por ejemplo, patrones inconsistentes entre medidas no financieras y medidas financieras, el uso excesivo de software bajo licencia y el uso de otro tipo de propiedad intelectual podría ser indicio de posible fraude.

Identificar potenciales esquemas de fraude y priorizar sobre la base de su riesgo

El fraude por definición implica mala conducta intencional diseñada para evadir la detección; por lo anterior, el equipo de evaluación de riesgo de fraude precisa realizar un razonamiento estratégico, con el fin de anticiparse tanto a los esquemas de fraude como a personas de dentro y fuera de la organización que pudieran estar en posición de perpetrar cada uno de tales esquemas. Un equipo de evaluación de riesgo de fraude está generalmente conformado por personas de la actividad de auditoría interna, finanzas, asesoría legal, tecnología de la información, seguridad y posiblemente otras funciones, dependiendo de la naturaleza de la organización.

El equipo de evaluación de riesgo de fraude identifica posibles esquemas fraudulentos utilizando lluvias de ideas, entrevistas a la gerencia, procedimientos analíticos y revisiones de fraudes previos. Durante este proceso, el equipo de evaluación de riesgo de fraude revisa las actividades y los esquemas relacionados con la industria, la ubicación y los programas de la organización, siempre considerando las características básicas del fraude (presión/incentivo, oportunidad y racionalización), preguntándose:

- 1. ¿Dónde existen oportunidades de fraude?
- 2. ¿Cuál es el nivel de presión al que está sometida la gerencia y que podría conducir a evadir los controles internos?
- 3. ¿Si la gerencia no cumple con las metas establecidas existen consecuencias?

Las áreas de fraude específicas deberían ser identificadas sin considerar la existencia y eficacia de controles internos (lo que se hace con posterioridad). La evaluación considera si el fraude podría ser cometido por un individuo solo o si requiere colusión entre empleados o personas externas a la organización. Los siguientes factores son considerados al priorizar el riesgo de fraude:

Impacto monetario	Impacto sobre la reputación de la organización	Pérdida de la productividad	Posibles acciones criminales/civiles, incluyendo posible incumplimiento regulatorio
Integridad y seguridad de los datos	Pérdida de activos	Ubicación y tamaño de las operaciones/unidades	Cultura de la organización
Volumen de negocios de gerentes/empleados	Liquidez de activos	Volumen o magnitud de transacciones	Tercerización

Mapeo de los controles existentes contra los potenciales esquemas de fraude e identificación de brechas

El equipo de evaluación de riesgo de fraude identifica los controles preventivos y detectivos implementados para afrontar cada riesgo de fraude y evaluar la probabilidad e impacto de cada posible fraude. Los controles antifraude a nivel de entidad, como una línea directa para recibir denuncias y una política de protección a denunciantes, así como una vigilancia del consejo, resultados de monitoreo continuo, código de conducta y el tono de las comunicaciones de la gerencia respecto de su tolerancia al riesgo de fraude son elementos importantes en este ejercicio.

El riesgo de que la gerencia eluda los controles tiene que ser considerado explícitamente y el costo/beneficio de controlar ese riesgo debería ser evaluado.

Probar la eficacia operativa de los controles para prevenir y detectar fraudes

La auditoría interna generalmente juega un papel importante en la evaluación de la eficacia operativa de los controles internos; los auditores internos no consideran solamente la existencia del control interno sino también

la eficacia del control interno por medio de pruebas periódicas de control. Por ejemplo, una organización podría implementar una política de seguridad con respecto a las claves de red, requiriendo que éstas sean cambiadas cada 30 días; sin embargo, los controles de acceso a la red no bloquean el acceso de un usuario si es que la clave no ha sido modificada según lo requerido y el control interno está presente, pero no es efectivo operativamente.

Documentar y reportar sobre la evaluación de riesgo de fraude

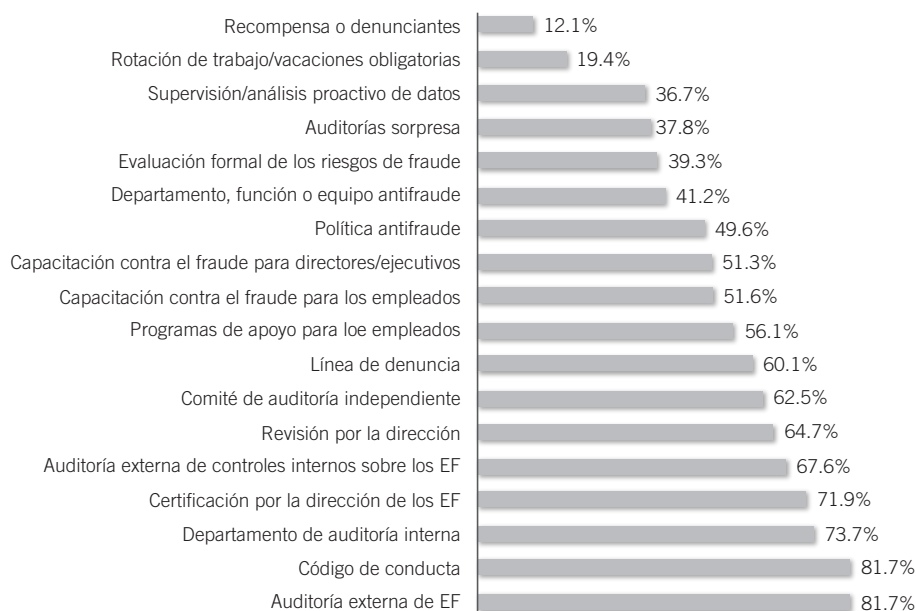
Las organizaciones necesitan documentar el proceso que identifica y evalúa el riesgo de fraude; los elementos clave que probablemente deberán documentarse como parte de una evaluación de riesgo de fraude para cada área importante de la organización incluyen:

1. Los tipos de fraude que tienen alguna oportunidad de ocurrir.
2. El riesgo inherente de fraude considerando la disponibilidad de activos líquidos y vendibles, la moral organizacional y la rotación de empleados, los antecedentes de fraudes y pérdidas y otros indicadores específicos de las áreas de la organización.
3. La idoneidad de programas antifraude que existan, su monitoreo y controles de prevención.
4. Las posibles brechas que se den en los controles de fraude de la organización, incluyendo la segregación de funciones.
5. La probabilidad de que se produzca un fraude importante.
6. El impacto que tendría un fraude sobre la organización.

Establecimiento de controles antifraude

Si bien, los controles no garantizan una protección total contra el fraude, establecerlos puede ayudar tanto a mitigar pérdidas como a disuadir a defraudadores potenciales; al aumentar la percepción de que los fraudes serán detectados, por lo que establecer controles internos específicamente diseñados para prevenir y detectar fraudes es una parte vital del programa de administración de riesgos de fraude. De igual manera existen controles antifraude que presentan una mayor efectividad que otros implementados, por lo que deberá evaluarse con frecuencia la viabilidad de su existencia; a continuación se presenta la frecuencia de existencia de cada uno de los controles antifraude; sin embargo, esto no indica su eficiencia y la probabilidad de que detecten un fraude o irregularidad.

Ilustración 17. Frecuencia de existencia de controles antifraude

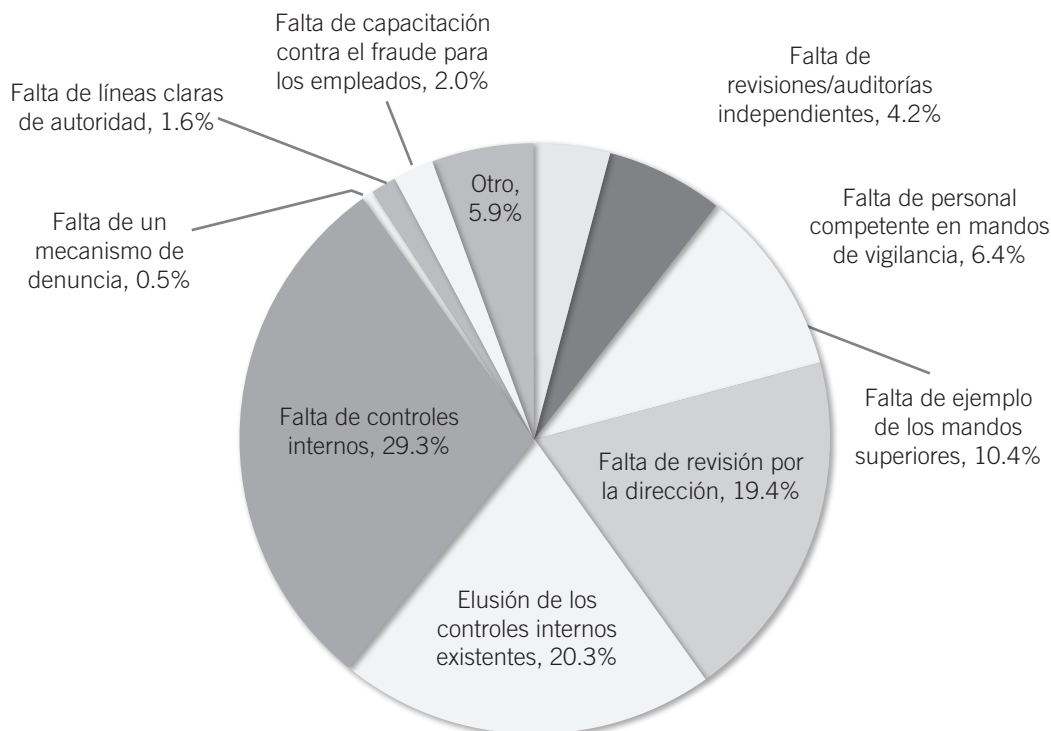


Fuente: Reporte a las naciones, ACFE, 2016.

La presencia de controles antifraude se correlaciona con menores pérdidas y detecciones más tempranas de fraude, las organizaciones que sufrieron fraudes y contaban con técnicas proactivas de análisis y supervisión de datos sufrieron pérdidas en un porcentaje de 54% menor y además detectaron el fraude en la mitad del tiempo que sus contrapartes sin estas técnicas. Es de llamar la atención que la auditoría externa a los estados financieros, al ser un control más implementado mantiene una correlación menor que el resto de los controles.

Adicional a estas características se han identificado cuáles son las principales causantes del fraude en las organizaciones relacionadas con el control interno. A continuación se presenta un gráfico de las principales debilidades que pudieran ocasionar o han ocasionado con mayor frecuencia los fraudes detectados.

Ilustración 18. Debilidades de control que contribuyen al fraude



Fuente: Reporte a las naciones, ACFE, 2016.

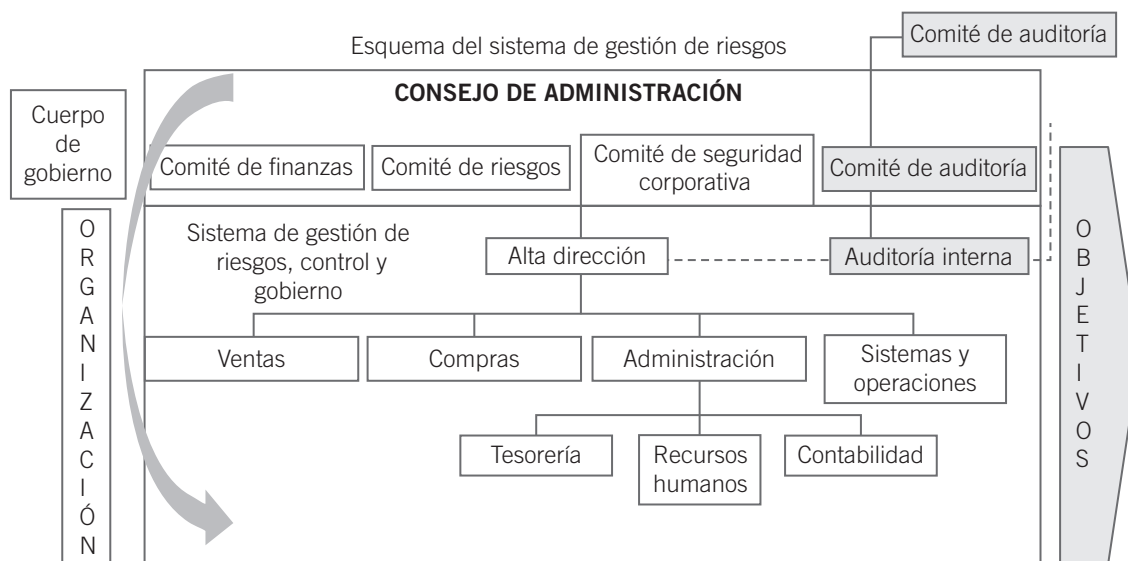
Un adecuado sistema de gestión de riesgos y controles corporativos en general, al igual que el riesgo de fraude en lo específico, permite a la organización contar con un mapa completo de los riesgos de fraude y tomar medidas oportunas para su prevención.

Por el contrario, el no contar con un esquema de evaluación constante e implementarlo de manera inadecuada, puede dar lugar a la ineficiencia del sistema y a la percepción por parte del consejo y la administración de ser una inversión innecesaria, dado que no cumple adecuadamente con su objetivo.

1.4.2 Responsabilidades del personal en la prevención y detección de fraude

El rol de supervisión y vigilancia de los procesos relacionados con la prevención, detección e investigación de fraude es llevada a cabo por diversas áreas dentro y fuera de la organización, siempre bajo la supervisión general y responsabilidad última del consejo de administración. El siguiente gráfico muestra un ejemplo de funcionamiento del sistema de gestión de riesgos de fraude en las organizaciones:

Ilustración 19. Esquema del sistema de gestión de riesgos



Fuente: Elaborado por el autor.

Consejo de administración

El consejo de administración tiene la responsabilidad de que exista un gobierno corporativo efectivo y responsable para afrontar los aspectos relacionados con el fraude; la función del consejo es vigilar y monitorear las acciones de la gerencia para gestionar los riesgos de fraude; asimismo, evalúa la identificación que la gerencia ha hecho de los riesgos de fraude, la implantación de medidas antifraude y la creación de los lineamientos para el manejo del riesgo de fraude.

Como el consejo constituye la más alta autoridad de la organización, es responsable de establecer los lineamientos para el manejo del riesgo de fraude dentro de la organización; el consejo puede implementar políticas que incentiven un comportamiento ético, incluyendo procesos destinados a empleados, clientes y socios de relaciones externas de negocios, motivándolos para que reporten instancias donde tales políticas hayan sido violadas. El consejo podrá monitorear la efectividad de la gestión de riesgos de fraude, designando a un miembro de nivel ejecutivo de la gerencia para que se responsabilice de la coordinación de la gestión de riesgos de fraude y para que reporte sobre la misma al consejo.

Para establecer el apropiado tono en la cima, el consejo necesita un esquema de gobierno adecuado. Esto abarca todos los aspectos de gobierno del consejo, incluyendo a los miembros independientes del consejo, quienes ejercen control sobre información de este último, agenda, acceso a gerencia y a asesores externos de la misma, así como a quienes cumplen independientemente con sus responsabilidades en los comités de nominación/gobierno, remuneración, auditoría y otros.

Comité de auditoría

Un comité de auditoría nombrado por el consejo de administración se convierte en los ojos y oídos independientes de los inversionistas y otras partes interesadas. El rol del comité es evaluar el trabajo de la gerencia en cuanto a la identificación de los riesgos de fraude y a la implementación de medidas antifraude; la tolerancia cero hacia el fraude en toda la organización es también un rol del comité.

El comité de auditoría contrata auditores externos para que se pronuncien sobre los estados financieros de la organización y proporcionen recomendaciones relacionadas con el control interno. Los auditores externos reportan al comité de auditoría y no a la gerencia. El comité de auditoría usualmente vigila las actividades de auditoría interna.

La norma IIA 2060 “Informe a la alta dirección y al consejo” establece que el comité de auditoría debe informar periódicamente a la alta dirección y al consejo sobre la actividad de auditoría interna en lo referido al propósito, autoridad, responsabilidad y desempeño de su plan. El informe también debe incluir exposiciones al riesgo y cuestiones de control significativas, asuntos de gobierno y otros más que son necesarios o requeridos por la alta dirección y el consejo.

El comité de auditoría es responsable de la supervisión de los controles para prevenir y detectar fraude gerencial; en este rol, el comité de auditoría es responsable de la supervisión del cumplimiento de la alta gerencia con respecto a la emisión de informes financieros apropiados; asimismo, el comité es responsable de evitar que la alta gerencia pase por estrictos controles o ejerza cualquier otra influencia inapropiada sobre el proceso de emisión de reportes.

Alta dirección

Ésta es la responsable de la supervisión de las actividades de los empleados y, generalmente, hace esto por medio de la implementación y monitoreo de procesos y controles internos; además, la gerencia evalúa la vulnerabilidad de la entidad frente a actividades fraudulentas. El fraude puede ocurrir en cualquier organización, pero el grado y detalle involucrados en la evaluación del riesgo podría ser proporcional al tamaño y complejidad de la organización.

La gerencia tiene la responsabilidad de establecer y mantener un sistema de control interno efectivo a un costo razonable; de igual manera, las discusiones de la gerencia con investigadores y consejeros legales cumplen un papel importante en el desarrollo de controles sobre el proceso de investigación; incluyendo la elaboración de políticas y procedimientos para realizar una eficaz investigación del fraude, así como para manejar debidamente los resultados de las investigaciones, sus informes y comunicaciones.

Auditoría interna

Los auditores internos evalúan los riesgos que sus organizaciones afrontan sobre la base de planes de auditoría ejecutados mediante pruebas adecuadas; la importancia que una organización preste a sus actividades de auditoría interna constituye un indicio del compromiso que tiene la organización con respecto a un efectivo control interno y manejo del riesgo de fraude.

Los auditores internos no son responsables de detectar todos los fraudes, pero siempre deben estar alerta ante la posibilidad de su existencia y brindar información suficiente para decidir si debe ser recomendada una investigación más profunda.

El Marco Internacional para la Práctica Profesional contempla las siguientes Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna en lo relativo al fraude, así como al rol del auditor interno en la detección, prevención y monitoreo de los riesgos de fraude y la manera de afrontar esos riesgos en las auditorías e investigaciones que se realizan.

La norma IIA 1200 “Aptitud y cuidado profesional” menciona que los auditores internos deben tener conocimientos suficientes para evaluar el riesgo de fraude y la forma en que se gestiona por parte de la organización, pero no es de esperar que tengan conocimientos similares a los de aquellas personas cuya responsabilidad principal es la detección e investigación del fraude.

Asimismo, respecto a su competencia, la norma IIA 1220 “Cuidado profesional” menciona que el auditor interno debe ejercer el debido cuidado profesional al considerar en la realización de su trabajo, la relativa complejidad, materialidad o significatividad de asuntos a los cuales aplican procedimientos de aseguramiento, la adecuación y eficacia de los procesos de gobierno, gestión de riesgos y control, la probabilidad de errores materiales, fraude o incumplimiento, el costo de aseguramiento en relación con los beneficios potenciales.

En la norma IIA 2120 también se establece que la actividad de auditoría interna debe evaluar la posibilidad de ocurrencia de fraude y cómo la organización maneja y gestiona el riesgo de fraude y en la 2210 “Objetivos del trabajo”, que el auditor interno debe considerar la probabilidad de errores, fraude, incumplimientos y otras exposiciones significativas al elaborar los objetivos del trabajo.

Los autores internos pueden realizar auditorías proactivas con el fin de encontrar casos de malversación de activos y de presentación de información falsa e incluir el uso de técnicas de auditoría asistidas por computadora; incluyendo la minería de datos con el propósito de detectar tipos particulares de fraude. Los auditores internos también pueden aplicar procedimientos analíticos y de otra índole que les permitan encontrar rubros inusuales y llevar a cabo análisis detallados de cuentas y transacciones de alto riesgo para identificar un posible fraude.

El rol de la auditoría interna en caso de que así lo decidiera el consejo y la alta dirección mediante el estatuto de auditoría, podría incluir la investigación inicial y exhaustiva de una sospecha de fraude, el análisis de la causa raíz del asunto, la formulación de recomendaciones para un mejor control, el monitoreo de una línea de denuncias, así como dirigir sesiones de capacitación en ética. Si tales funciones les han sido asignadas, la auditoría interna tiene la responsabilidad de obtener las destrezas y competencias necesarias, incluyendo el conocimiento de esquemas de fraude, técnicas de investigación y leyes pertinentes.

Auditores externos

Los auditores externos de la organización tienen la responsabilidad de cumplir con las normas profesionales y planificar y ejecutar la auditoría de los estados financieros de la organización, con la intención de obtener seguridad razonable de que los estados financieros se encuentran libres de distorsiones materiales y si estas últimas han sido ocasionadas por error o fraude. Cuando el auditor externo ha determinado que hay evidencia de un posible fraude, las normas profesionales de auditoría externa requieren que el asunto sea comunicado a un nivel gerencial apropiado. El fraude que involucra a la alta dirección generalmente es reportado por el auditor externo de manera directa a quienes están a cargo del gobierno corporativo de la organización como, por ejemplo, el comité de auditoría.

Investigadores de fraude

Éstos son usualmente responsables por la detección e investigación del fraude, la recuperación de activos y desempeñan también un rol en la prevención del fraude. La alta dirección y el comité de auditoría precisan respaldar a los investigadores para permitir que todas las partes interesadas sepan que la organización está preparada para responder, rápida y apropiadamente, ante los riesgos de fraude.

La ubicación de una unidad de investigación de fraude dentro de una organización puede variar, esto de acuerdo con sus funciones y atribuciones en la organización respecto a la detección de fraude. La unidad de investigación de fraude puede ser parte de un departamento de seguridad corporativa, que trabaje estrechamente con los auditores internos o que se involucre en las actividades de auditoría interna, de modo que los empleados de la unidad de investigación de fraude tengan acceso a los hallazgos de los auditores internos independientes.

Los investigadores de fraude con frecuencia trabajan estrechamente con asesoría legal para iniciar los procesos legales contra los perpetradores y es probable que las comunicaciones que se crucen entre investigaciones de fraude y la asesoría legal se consideren como confidenciales, lo que permite un diálogo libre y abierto. Además, el trabajo de un investigador de fraude que haya sido realizado con la orientación de la asesoría legal podría constituir un producto del trabajo de los abogados sujeto a protección.

El investigador líder usualmente determina cuáles son los conocimientos, destrezas y demás competencias que se precisan para llevar a cabo la investigación de manera efectiva y designa a personas competentes y apropiadas para que formen parte del equipo; dicho proceso podría incluir el asegurarse de que no existan posibles conflictos de intereses con quienes están siendo investigados o con cualquier otro empleado de la organización.

Asesoría legal

Los roles y responsabilidades de la asesoría legal interna están frecuentemente regulados por las leyes de cada jurisdicción; por lo general, un abogado actúa en el mejor interés de la organización y también debe preservar la confidencialidad del cliente; el descubrimiento de un fraude puede hacer que estos dos deberes éticos entren en conflicto.

Al verse frente a integrantes de una organización quienes tienen intención de cometer fraude, un abogado puede apremiarlos para que lo reconsideren y asesorarlos para que busquen una opinión legal distinta, así como referir el tema a una autoridad superior dentro de la organización.

La asesoría legal interna podría decidir renunciar luego de conocer sobre un posible fraude o que éste se esté realizando de manera continua, especialmente si se quiere hacer uso del trabajo de la asesoría legal para realizar o mantener el fraude. Si es que el asesor legal renuncia, éste o el asesor externo pueden documentar las medidas tomadas para notificar a los miembros de la organización que están actuando mal con respecto a:

1. La ilegalidad de su conducta actual o intencional.
2. Las consecuencias de tal conducta.
3. El intento del asesor para disuadir dicho comportamiento.

Otros empleados

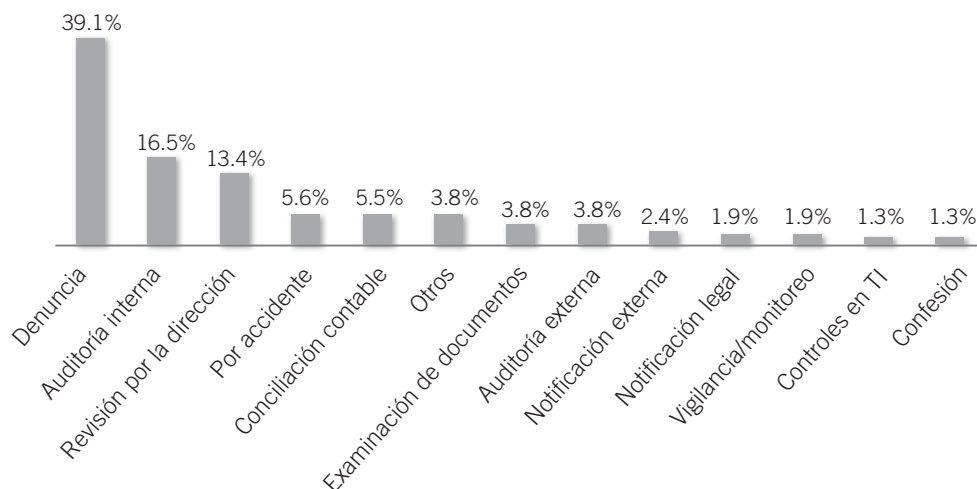
Cada empleado cumple una función en la prevención y detección de fraude, los empleados son los ojos y oídos de la organización, ellos deberían estar facultados y tener los medios para mantener un lugar de trabajo donde se respeten los valores éticos y las políticas organizacionales. Los empleados pueden reportar sospechas de fraude a una línea de denuncias de fraude accesible a ellos, al departamento de auditoría interna y a un miembro de la gerencia.

Para el adecuado funcionamiento del sistema de prevención, detección y disuasión del fraude es necesario que todos los miembros de la organización comprendan su rol dentro del mismo y mantengan adecuadamente los controles establecidos para tales fines; asimismo, deben reportar cualquier sospecha o anomalía que detecten durante el ejercicio de sus funciones.

1.4.3 Métodos de detección de fraude

ACFE en el Reporte a las naciones 2016 publica los métodos identificados como más comunes para la detección inicial de fraude, mismos que deberán ser contemplados en un eficiente programa para la prevención de fraude en la organización. Estos métodos brindan una importante guía para identificar qué programas son más eficientes y útiles, y en los cuales se deberá realizar una mayor inversión, ya que representan un costo muy alto para la organización sin reportar beneficios adecuados.

Ilustración 20. Métodos de detección de fraude ocupacional



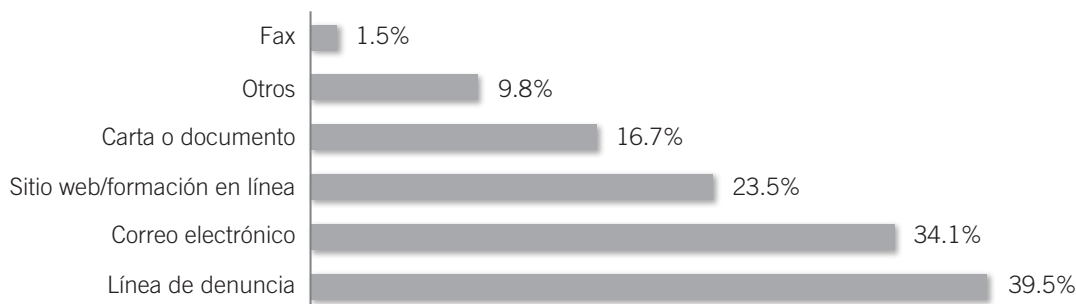
Fuente: Reporte a las naciones, ACFE, 2016.

Se ha identificado que las denuncias como principal método de detección de fraude deben ser el foco de atención de las organizaciones. De las denuncias, 51.5% provienen de empleados de la organización; 40% de las denuncias provienen de personas distintas a los empleados, 17.8% de las ocasiones de los clientes y 9.9% de los proveedores son fuentes relevantes de denuncias, por lo que se les debe dar a conocer los mecanismos relevantes (ACFE, 2016).

De igual manera, 14% de las denuncias provienen de fuentes anónimas, por lo que hacer obligatoria la identificación del denunciante durante el proceso de denuncia puede disminuir la detección de casos.

Las denuncias se presentan por diversos medios, siendo la llamada telefónica la más común y el e-mail o medios electrónicos es la segunda en frecuencia de uso; estos datos pueden interpretarse para la implementación de un sistema de detección de fraude, debido a que un mayor número de herramientas y medios para la denuncia dan como resultado el aumento del índice de detección.

Ilustración 21. Medios de denuncia



Fuente: Reporte a las naciones, ACFE, 2016.

La detección de fraude puede realizarse con la aplicación de una auditoría forense que permita realizar una investigación sobre la presunción de los ilícitos, es difícil que las organizaciones puedan eliminar el riesgo de fraude porque siempre hay personas que están motivados para cometerlo; una oportunidad puede surgir en cualquier momento a cualquier persona de la organización para anular los controles internos y coludirse con otros.

Aunque cada organización es susceptible al fraude, en la mayoría de las ocasiones no es rentable tratar de eliminar todo riesgo cuando el costo de diseñar, implementar y monitorear los controles internos contra el mismo supera la estimación del impacto del riesgo, así como el costo y la eficiencia de los medios de detección de fraude son factores que deben considerarse para el diseño del sistema antifraude.

1.4.4 Política de ética organizacional y política antifraude

Para comprender y valorar la oportunidad de ocurrencia de fraude en una organización, es necesario obtener una comprensión de la cultura corporativa, la cual proporciona una visión holística e integral de la filosofía de la gestión y el entorno de control. Si bien, el cultivo de una cultura ética es crítico como primer paso, reducir el riesgo de fraude también requiere entrenamiento y educación, políticas fuertes y procedimientos encaminados a gestionarlo.

La ética es el mayor elemento de la gobernanza, se refiere a aquellos principios de conducta deseada que, de manera consensuada, se consideran como comportamiento aceptable. Está conformada por un conjunto de valores que son las reglas bajo las cuales un individuo decide qué es bueno y qué es malo, qué debe y qué no debe hacer.

El consejo o cualquier otro órgano de gobierno designado es el encargado de promover valores éticos, los gerentes administrativos definen el clima ético en sus áreas y los estándares éticos varían en cada cultura, por lo que las organizaciones globales deberán decidir cómo adaptarán sus estándares globales. A continuación se enlistan algunos factores que pueden llegar a causar comportamientos en contra de la ética:

1. Presiones para mejorar el desempeño a corto plazo.
2. Énfasis en la estricta adherencia a la autoridad jerárquica.
3. Lealtades de grupos de trabajo informales.
4. Procesos de decisiones de un comité que pueden hacer imposible abstenerse o evitar obligaciones éticas.

5. Presión de la competitividad externa.
6. Comportamiento ilegítimo de otros.

Otras posibles causas son las siguientes:

1. La dirección recompensa conductas inadecuadas.
2. Objetivos y expectativas poco razonables.
3. Compensaciones e incentivos no vinculados con el comportamiento ético.
4. Falta de responsabilidad organizacional.
5. La atención está puesta en los resultados finales y de corto plazo, mas no en el largo plazo.
6. La gente está enfocada en sus propios objetivos y no en los de la organización.

El establecimiento de una cultura ética en la organización deberá contar con las siguientes características:

1. Fundada en una buena gobernanza.
2. Creada por medio de un robusto programa de ética.
3. La ética del negocio es el mayor elemento del gobierno corporativo.
4. La gerencia es la principal responsable de promover y dar el ejemplo de comportamiento ético; la importancia del tono en la dirección no debe ser subestimado.
5. La ética del negocio es la conciencia de qué comportamiento es permitido y aceptado en la organización en particular.
6. Los métodos específicos que la gerencia usa para promover el comportamiento ético puede variar de acuerdo con la organización, su ambiente y madurez en el tema.
7. El código de ética es el sistema de valor general que la organización desea aplicar a las actividades de sus miembros.

Los beneficios de contar con un código de ética son:

1. Comunica efectivamente los valores aceptables a todos los miembros.
2. Brinda un método de políticas y disciplina para miembros.
3. Establece normas contra las cuales los individuos pueden medir su desempeño.
4. Comunica el sistema de valor al exterior de la organización.

Para elaborar un código de ética institucional, la organización deberá realizar el siguiente procedimiento:

1. Identificación de objetivos de la empresa y alineación con la misión y visión.
2. Redacción conjunta del código entre la empresa o entidad pública y asesores externos.
3. Definición de términos integrales.
4. Información y capacitación al personal.
5. Revisión periódica.

También deberá tener algunas consideraciones específicas para que una vez establecido se pueda monitorear su cumplimiento e imponer sanciones en caso de incumplimientos:

1. Creación de un comité encargado de la implementación de la cultura ética.
2. Monitoreo del cumplimiento e implementación de las medidas disciplinarias definidas.
3. Definición del mecanismo de comunicación, reporte y toma de decisiones respecto a la aplicación del código de ética y conducta.

4. Definición de políticas y procedimientos.
5. Seguimiento de las reglas de operación del comité.
6. Apoyo del área de auditoría interna para la revisión periódica.

Algunos de los métodos que la organización puede implementar para la evaluación de la política y código de ética incluyen:

1. Revisión de la ética relacionada con políticas y procesos en toda la organización.
2. Auditorías de funciones específicas relacionadas con la ética, como es la función de cumplimiento.
3. Una encuesta sobre ética a los empleados de la organización.
4. Una evaluación informal del clima ético en la organización y un proyecto de evaluación de riesgos de ética.

Para que la política de ética y el código funcionen adecuadamente, es necesario que las siguientes áreas cuenten con las atribuciones responsables del clima ético en la organización:

Consejo de administración	Alta dirección	Administración operacional
Está a cargo de la supervisión del clima ético. Los auditores internos experimentan este clima, pero sin perder su independencia.	Es el principal responsable de promover el comportamiento ético. Sus métodos pueden variar dependiendo del ambiente y la madurez de la organización.	Está a cargo de la supervisión del clima ético. Los auditores internos experimentan este clima, pero sin perder su independencia.
Demás empleados	Terceras partes	Auditoría interna
Se debe motivar a todos los individuos a seguir los estándares de ética.	- Entendemos por terceras partes a proveedores, vendedores, agentes y clientes. - Las acciones de éstos pueden poner en riesgo la reputación de la organización.	- La organización confía en que cuenta con un alto nivel de integridad y ética. - El director ejecutivo de auditoría tiene una conducta proactiva. - Debe asistir a la organización de manera periódica.

La capacitación acerca de las conductas antiéticas y el fraude es un factor clave en la prevención y disuasión de los mismos; la capacitación comunica expectativas de la organización acerca de la conducta de los empleados, los procedimientos y las normas necesarias para implementar controles internos, funciones y responsabilidades de los empleados para informar la mala conducta.

Los empleados necesitan entender el comportamiento ético que se espera de ellos y que actúen en consecuencia dentro de la organización; en el transcurso de la inducción a nuevos empleados se deben presentar la misión, valores de la organización y el código de conducta, así como los tipos posibles de fraude y la responsabilidad de informar de posibles violaciones de ética, conducta y decoro. De igual manera pasará con los detalles de la línea de emergencia y otras formas de denunciar posibles fraudes.

La capacitación acerca de fraude debe impartirse de acuerdo con la posición del empleado en la organización, también puede utilizarse como autoevaluación de riesgos e incluso para disuadir a los que probablemente asistan y estén cometiendo fraude, informando que cualquier acto será detectado por medio del sistema de gestión de riesgos y tendría graves repercusiones para los involucrados. La capacitación continua a lo largo de la carrera

de un empleado refuerza la concientización de fraude y el costo de este último a la organización. Independientemente del método utilizado para producir y difundir el material de capacitación, un objetivo fundamental es poner a prueba la comprensión del empleado con la capacitación de fraude; lo anterior se puede realizar por medio de encuestas en línea que no sólo confirman asistencia, sino que también ofrecen exámenes rápidos para determinar si los empleados han adquirido los conocimientos necesarios provenientes de la capacitación.

El sistema de prevención, detección y disuasión de fraude, como se explicó con anterioridad, es una red de controles, políticas y acciones que blindan a la organización contra estos ataques; es de gran relevancia que todos los miembros comprendan el tema y su rol dentro del sistema, sólo de esta manera se podrán prevenir y detectar, de forma oportuna, los fraudes. La auditoría forense representa un control que puede ser preventivo o detectivo, dependiendo del momento en que se implemente, se tienen una serie de herramientas que permiten a los auditores cumplir su rol dentro del proceso de la organización.

1.5 Evaluación del riesgo de fraude

1.5.1 Formas de enfrentar un fraude

Existen dos formas fundamentales de enfrentar una situación de fraude:

1. Investigar el fraude utilizando un enfoque pasivo o controles internos de evaluación. El enfoque depende de cómo detecten los auditores las banderas rojas; aunque algunos programas de auditoría incluyen banderas rojas obtenidas por medio de la observación de auditoría, se espera que los auditores, mediante su experiencia profesional, adquieran habilidades de detección y observación de las banderas rojas.
2. Reaccionar a las acusaciones recibidas por medio de un denunciante u otro medio de auditoría, siendo éste el medio más frecuente con el que se detectan fraudes.

Históricamente, la profesión se ha dedicado a evaluar la adecuación y efectividad de los controles internos para detectar el fraude; los auditores documentan primero el sistema de control interno. Para brindar aseguramiento de que los controles son adecuados, los ponen a prueba para determinar si operan como es debido, con base en una muestra aleatoria de las transacciones registradas en el sistema.

Convencionalmente, las normas establecen que los auditores deben estar alerta a las banderas rojas de fraude durante la realización de una auditoría. Varios estudios indican que la falta de escepticismo profesional es la principal causa para la falla de la auditoría al detectar fraudes.

Este capítulo se enfoca en cómo utilizar la auditoría forense para detectar estas prácticas en los sistemas de las principales áreas del negocio u organización; la auditoría forense es un enfoque proactivo de auditoría diseñada para responder al riesgo de fraude. Esencialmente, la auditoría forense requiere que se responda a las siguientes preguntas:

1. ¿Quién cometió el fraude y cómo?
2. ¿Qué tipo de fraude estamos buscando?
3. ¿El fraude debería ser visto como un riesgo inherente?
4. ¿Cuál es la diferencia entre los controles internos y la oportunidad de fraude?
5. ¿Cómo es justificado el fraude?
6. ¿Cómo podemos incorporar la teoría del fraude en nuestro enfoque de auditoría?
7. ¿Cuáles de las maneras de hacer la auditoría forense pueden utilizarse para detectar el fraude?

Los pasos o fases a seguir en una auditoría forense son los mismos que en una auditoría tradicional; sin embargo, lo que la hace diferente es simplemente el cuerpo de conocimientos asociados con el fraude. La teoría de fraude deberá ser construida durante el curso de la auditoría; especialmente, durante la ejecución de la auditoría, los

auditores deben determinar el tipo y tamaño del riesgo de fraude. Para desempeñar una evaluación de riesgo de fraude, éste es asociado con los principales sistemas de negocio. En la auditoría tradicional el riesgo se relaciona con los controles, sin embargo, en este caso es dirigido al riesgo de fraude. Al incorporar la teoría de fraude en la evaluación de riesgo de fraude, las estrategias de ocultación realizadas por el perpetrador también son puestas en consideración. Los principios de la teoría del fraude son los siguientes:

1. La teoría de fraude es un cuerpo de conocimiento.
2. El fraude es predecible en la extensión de cómo éste ocurrirá en una situación específica, no necesariamente en la ocurrencia actual.
3. La clave para localizar el fraude es observar dónde ocurre.
4. Si quieres reconocer el fraude, necesitas conocer cómo se ve o qué características tiene cada esquema de fraude.
5. Las personas cometen fraude, no los controles internos.
6. Los riesgos de fraude y controles de riesgo tienen similitudes; sin embargo, el riesgo de fraude difiere del riesgo de control, ya que contiene los elementos de intención y ocultamiento.
7. El procedimiento de auditoría forense debe ser diseñado para descifrar las estrategias de ocultación asociadas al esquema de fraude.
8. Los procedimientos de auditoría forense deben validar el monto o significatividad económica de la transacción.
9. Los comentarios de auditoría forense difieren del informe regular de auditoría interna.

Los auditores que trabajan en el área de auditoría forense necesitan:

1. Estar alertas de la existencia de banderas rojas de fraude.
 - a) Estrategias de ocultación de fraude.
 - b) Sofisticación en la ocultación del fraude.
 - c) Indicadores de transacciones fraudulentas.
2. Conocer la teoría que les provea una comprensión de cómo ocurre el fraude en un ambiente de negocios.
 - a) Definiciones de fraude.
 - b) El triángulo del fraude.

La metodología empleada en el diseño de un programa de auditoría de fraude consiste en las siguientes etapas:

1. Definir el alcance de la auditoría de fraude.
2. Verificar el cumplimiento con las normas profesionales aplicables.
3. Desarrollar la evaluación del riesgo de fraude que incluya:
 - a) Identificar el tipo de riesgo de fraude.
 - b) Identificar los procesos de negocio o riesgos contables.
 - c) Los controles internos están relacionados con el riesgo de fraude.
 - d) Las estrategias de ocultación para el esquema de fraude específico.
 - e) Desarrollar un plan de muestreo para investigar un esquema de fraude específico.
 - f) Desarrollar procedimientos de auditoría apropiados.
4. Escribir el reporte de auditoría forense.

5. Comprender el ciclo de conversión del fraude.
6. Desempeñar la investigación de fraude.

Lo primero con lo que el auditor debe contar para realizar una auditoría forense es con el conocimiento de la teoría de fraude, de tal manera que pueda tener conciencia acerca de la ocurrencia de algún acto de violación de integridad.

Una definición completa acerca del fraude incluye que es un acto cometido por una fuente interna o externa, siendo éste intencional y planeado. Los actos son ilegales típicamente y denotan un mal acto, como por ejemplo en los casos de declaración errónea de los estados financieros, violación de las políticas, lapsus ético y un problema de percepción. El acto causa una pérdida de fondos de la compañía, su valor o reputación, o cualquier beneficio no autorizado que es recibido personalmente o por otros.

Una vez que este concepto es comprendido como parte de la teoría, deberá comprenderse también el triángulo del fraude.

Este último es generalmente aceptado como parte del proceso de identificar y evaluar el riesgo de fraude. El concepto es simple, éste incluye que para que el fraude exista se requiere la existencia de racionalización, presión y oportunidad.

1. **Racionalización.** Es una decisión consciente realizada por el perpetrador para colocar sus necesidades por encima de las de los otros. El proceso de decisión ética varía por individuo, cultura y experiencia. La habilidad para identificar la racionalización varía de persona a persona durante el proceso de auditoría, por el hecho de que la organización está compuesta por un número de individuos. Por lo tanto, en una organización o un nivel departamental, las cuestiones que influyen en los individuos son fáciles de determinar.
2. **Presión.** Son los eventos que ocurren con la organización o en la vida individual de la persona, la presión varía a nivel global como factor de riesgo. Con la presión, las necesidades individuales del individuo se convierten en más importantes que la ética organizacional o sus objetivos.
3. **Oportunidad.** Para cometer un fraude, un individuo puede tener acceso a los activos o ser responsable de gestionar un proceso de control relacionado con la comisión del esquema de fraude. Tanto la posición de la persona como sus responsabilidades y autorización también contribuyen a la oportunidad de cometer fraude. Existe una correlación directa entre la oportunidad de cometer fraude y la capacidad de encubrirlo. Al evaluar el riesgo de fraude, los auditores necesitan considerar la oportunidad y capacidad para realizar el fraude, al diseñar el plan de auditoría.

Existen seis premisas que deberían ser comprendidas y aplicadas en los conceptos del triángulo de fraude:

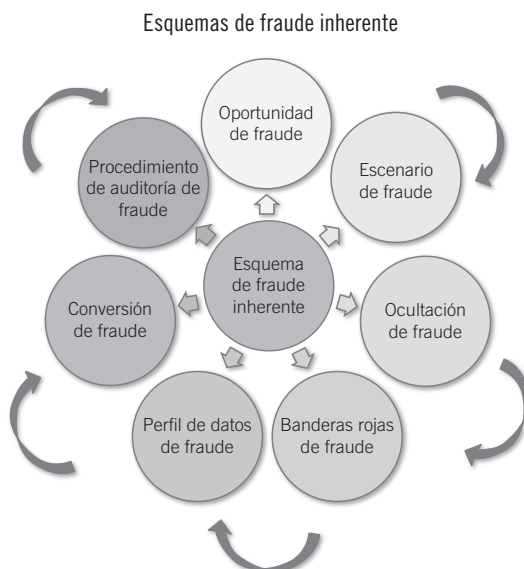
1. Los tres elementos del fraude (racionalización, presión y oportunidad) coexisten a diferentes niveles en cada individuo.
2. Los elementos del fraude se basan en las circunstancias de las personas.
3. La fuerza de un elemento puede causar que un individuo cometa un acto de fraude.
4. La fuerza de un elemento puede eliminar la preocupación por ser detectado.
5. Identificar los tres elementos es más fácil que medir los tres elementos.
6. Los factores de riesgo de fraude pueden ser originados por fuentes internas o externas.

Metodología

La metodología dirige el alcance de la auditoría forense al subsecuente diseño de la evaluación de riesgo de fraude. El primer propósito de la evaluación de riesgo de fraude es identificar los riesgos de fraude más probables y de mayor impacto para la organización. El proceso de evaluación clasifica los esquemas de fraude por función organizacional.

Por ejemplo, para desarrollar una evaluación de riesgo de fraude en toda la empresa se deben seguir los siguientes pasos:

1. Crear una clasificación de fraude para toda la empresa.
2. Identificar el tipo de fraude que se asocia con la clasificación de fraude para toda la empresa.
3. Delimitar las principales unidades operativas de la organización, por ejemplo, subsidiarias o departamentos de la compañía.
4. Delimitar los principales sistemas de negocio de la compañía o cuentas en la unidad operativa, por ejemplo, compras o ventas.
5. Identificar los esquemas de fraude inherentes que están relacionadas con una cuenta específica o un sistema de negocio.
6. Determinar la variación de los esquemas de fraude inherente, esto ocurre al nivel de proceso del negocio.
7. La variación del esquema de fraude está relacionada con la oportunidad de cometerlo. Esto se refiere a un escenario de fraude.



Fuente: Elaborado por el autor.

El círculo del fraude ilustra la relación en la teoría del fraude y el concepto de respuesta al fraude, y la auditoría de fraude muestra cómo un esquema de fraude inherente está ligado a una respuesta al fraude apropiado.

1.5.2 Consideraciones acerca de la oportunidad de fraude

La fase de oportunidad de fraude inicia con una lista de los esquemas de fraude que los individuos pueden cometer por la virtud de su posición en la organización. Esto puede notarse en los fallos en los procesos de control que crean una oportunidad para cometer el fraude en lugar de actuar como inhibidores.

El fraude ocurre porque los individuos usan sus posiciones para violar los controles intencionalmente. Esto puede suceder a cualquier nivel que tenga acceso al control, por ejemplo, a un nivel de empleado, supervisor o de gerencia. Esto puede ser perpetrado por una persona o un grupo de personas coludidas.

Asimismo, el fraude puede darse cuando no se han establecido controles para cierto proceso. Esta violación es un fallo de la gerencia para identificar oportunidad del riesgo de fraude y los posibles esquemas derivados. Comprendiendo la oportunidad de fraude, ayuda a los auditores a identificar qué esquemas pudieran cometerse y

cómo puede ocurrir el riesgo de fraude. Los auditores deben considerar, durante su trabajo, la sofisticación con la que el individuo cometió el fraude. Un enfoque del perfil individual es comprender la experiencia que tienen al cometer el fraude y qué los motiva a hacerlo. Los perpetradores de fraude en una organización pueden ser clasificados en cuatro grupos:

1. **Perpetradores por primera ocasión.** Son aquellos que no tienen un récord de actividad criminal y tienen una presión en sus vidas que hace que su capacidad de racionalizar sus comportamientos crea que son justificables.
2. **Perpetradores reincidentes.** Las estadísticas indican que las personas que cometen fraude interno tienen una alta tendencia de cometer un crimen más de una vez. En este sentido, la presión y la racionalización son aspectos de la teoría que será menos dominante que un ofensor por primera ocasión.
3. **Grupos de crimen organizado.** Estos grupos consisten en profesionales del fraude, que son internos o externos a la organización. Por lo general son grupos de profesionales en fraude o, en algunas ocasiones, de individuos que se especializan en un tipo particular de crimen. El factor principal es la oportunidad de cometer el crimen. Estos grupos pueden cometer crímenes tomando ventaja de la debilidad de los controles internos, extorsionando o presionando a los empleados o por medio de la colusión con vendedores o clientes.
4. **Cometidos internamente para el beneficio de la organización.** Este tipo de crimen es cometido usualmente por empleados que creen que el acto es por el bien de la compañía. Típicamente, la presión y racionalización por estos empleados es similar a quienes son ofensores por primera vez o quienes han repetido el crimen.

Comprender la experiencia individual de crimen y la motivación es el ingrediente clave para prevenir y detectar el fraude. El temor a la detección es visto por la gerencia como un medio para detener la comisión del mismo.

1.5.3 La auditoría forense

Hay tres enfoques para una auditoría forense: el pasivo, el reactivo y el proactivo; los auditores que toman el enfoque proactivo son quienes investigan los fraudes que aún no han sido realizados. La auditoría forense debe ser utilizada como una respuesta completa al riesgo de fraude, es en sí misma la aplicación de procedimientos para incrementar la posibilidad de identificar el fraude.

Los auditores pueden detectar el fraude mediante la prueba de los controles y observando las banderas rojas o los procesos de auditoría por sí mismos diseñados para investigar fraudes. A continuación se describen los tres tipos de enfoques:

1. **Pasivo.** La auditoría es diseñada para determinar que los controles han sido implementados y son operados por la gerencia. El proceso de muestreo es aleatorio. El proceso de auditoría es diseñado para determinar la existencia de los controles y para estar alerta de las banderas rojas de fraude.
2. **Reactivo.** En el enfoque reactivo, es desarrollada una investigación en respuesta a las declaraciones de fraude. En este enfoque, los procesos se enfocan en resolver la declaración específica.
3. **Proactiva.** En este enfoque, la investigación por fraude toma lugar cuando aún no existe una declaración o aviso de fraude, o incluso cuando no existe ningún fallo en controles que sugieran que un fraude está ocurriendo.

1.5.4 Responsabilidad de los auditores ante el fraude

En una auditoría tradicional, los auditores tienen la responsabilidad de estar alertas a las señales de fraude o *banderas rojas*, esto mediante conocer cuáles son las áreas o transacciones de cada operación que son susceptibles a fraude y la manera más común en cómo se perpetran. A continuación se presenta un ejemplo de lo que podrían ser señales de alerta en las facturas de proveedores y su clasificación:

Banderas rojas de facturas del proveedor						
Nombre de la compañía						
Unidad de riesgo: Banderas rojas en facturas de proveedores						
Tipo de bandera roja	Condición e información de documento	Consideraciones de control interno	Consideraciones de transacciones	Procesamiento o grabación	Otros	
Anomalía	Copia vs original	Retorno de cheque o retenido para la gerencia	Consistencia en el patrón de facturación	Documentación retenida en archivo no pagadero	Ejecutivo relacionado con montos pequeños	
Imprecisión	Falta de una descripción clara del producto y la calidad	Muchas facturas aplicadas para abrir una orden de compra	Ninguna	Cargo en un alto volumen contable	Nombre del vendedor	
Restricción	Sin número telefónico del proveedor o dirección física	Proveedor usado sólo por un gerente	Ninguno	Pagado el mismo día en que ingresa a cuentas por pagar	Todas las preguntas enviadas al vicepresidente	
Pérdida	Inexistencia de la orden del cliente e inexistencia de la factura del proveedor	Sin orden de compra o reporte de recepción	Ninguna dirección de envío de información	Ninguno	Ninguno	
Ilógico	Proveedor sin sitio web, tipo de papel inconsistente y consistencia con las expectativas	Aprobación incorrecta	Números de factura secuenciales o números de factura que no se encuentran en orden de fecha	Fecha de orden de compra después de fecha de factura	Consistente incluso en los montos	
Frecuencia	Ocurrencia de facturas no consistente con las expectativas	Monto de la factura del proveedor mayor a la orden de compra	Ninguno	Preguntas del gerente acerca del estatus de pago	Montos pequeños por debajo del umbral de control	
Rango	Ninguno	Montos de factura consistentemente por debajo del umbral de control	Número de factura de proveedor limitado o muy grande	Ninguno	Patrón de gasto excesivo	
Cambio	Variaciones en el formato y estilo de las facturas	Dirección o cuenta de banco; aumento de presupuesto en la línea de gastos	Ninguno	Transferencia periódica de cargos	El cambio del proveedor se correlaciona con el cambio de administrador o evento	
Error	Impuestos por ventas o impuesto al valor agregado incorrectos	Las facturas no coinciden con los registros	Los números de control son registrados en el sistema incorrectamente	Registrado en las cuentas inapropiadas	Pagos duplicados	
Aritmética	Los cargos no son totales	Ningún control independiente de las cuentas o saldos	Ninguno	Ninguno	Cálculo inapropiado de los impuestos o cargos adicionales	
Inusual	Cargos adicionales atípicos para la industria	Cargos adicionales por escrito	Factura u orden de compra contiene letras o símbolos especiales que no se encuentran en los documentos	Instrucciones especiales por escrito	Uso de software para pequeñas empresas para crear la factura	

En el plan de auditoría deberá construirse una matriz que permita identificar las banderas rojas durante el proceso del mismo.

1. Determinar el esquema de fraude específico y la variación del esquema de fraude.
2. Identificar la oportunidad de cometer el esquema de fraude, de este modo desarrollar los escenarios de fraude.
3. Relacionar las estrategias de ocultación posibles con el esquema de fraude específico.
4. Identificar las banderas rojas por medio de un evento que puede ser observado y medido por el auditor.
5. Relacionar la bandera roja con la estrategia de ocultación.
6. Identificar la bandera roja o evento desencadenante, que llevará al auditor a desarrollar procedimientos adicionales.
7. Derivar todas las posibles conclusiones.

Ejemplo:

1. Un esquema de fraude inherente en el proceso de compra se refiere a un proveedor favorecido.
2. Una variación y la estrategia de ocultación en el esquema de proveedor favorecido es evitar las ofertas usando el concepto de compra agregada.
3. El esquema opera indicando en la solicitud de propuestas que serán compradas 1,000 unidades. Sin embargo, la intención real es comprar 10,000 unidades. El vendedor favorecido recibe la información anticipadamente de la verdadera intención de compra, lo que le favorece el poder ofrecer un precio menor que los competidores con la certeza de obtener mejores ganancias.
4. La bandera roja es cuando las compras reales exceden la solicitud de la propuesta por un importe umbral. Para ilustrar, si las compras reales a lo largo de un periodo de 12 meses superan la cantidad en 20%, se trata de una bandera roja de la ocurrencia del esquema de fraude. El auditor necesitaría llevar a cabo procedimientos adicionales para determinar si la adquisición sabía o debería haber sabido que la compra real excedería el monto de la solicitud de propuesta.
5. Los auditores pueden llegar a tres posibles conclusiones:
 - a) Ninguna bandera roja fue observada.
 - b) Una bandera roja observada fue resuelta. Por lo que no existen banderas rojas aparentes.
 - c) Se observó una bandera roja y no se resolvió. La bandera roja no se resolvió mediante procedimientos de auditoría adicionales y la transacción se identificó como una transacción sospechosa que justificaba una investigación.

De este modo puede decirse que la auditoría forense consiste en 10 pasos:

1. Identificar el esquema de fraude inherente.
2. Identificar las variaciones en los diferentes esquemas de fraude.
3. Identificar las estrategias de ocultamiento y las banderas rojas asociadas.
4. Identificar oportunidades de fraude.
5. Desarrollar un escenario de fraude.
6. Construir un perfil de datos del esquema de fraude.
7. Usar técnicas de minería de datos para investigar las transacciones consistentes con el perfil de datos.
8. Diseñar el procedimiento de auditoría.
9. Considerar la suficiencia, rentabilidad y autenticidad de la evidencia recabada.
10. Formular una conclusión de fraude.



La base de la auditoría forense que se diferencia de la auditoría tradicional es la siguiente:

1. La auditoría forense no es una prueba de la existencia de controles.
2. La auditoría forense no confía o se basa en la información de la gerencia y asume falsificaciones en la información existente.
3. La auditoría forense afirma la autenticidad de la transacción.
4. Con la auditoría forense se puede llegar a dos conclusiones:
 - a) No hay evidencia conocida de fraude que resulte en evidencia indirecta de que el control está operando.
 - b) Una transacción sospechosa es identificada, por lo que existe evidencia de fraude.

A continuación se presenta un ejemplo de esquema de fraude por empleado fantasma, con las estrategias o procedimientos para determinar la existencia del fraude.

Apropiación indebida de activos: Empleado fantasma					
Nombre de la organización					
Matriz de la teoría de fraude y auditoría de fraude					
Unidad de riesgo: Apropiación indebida de activos: Empleado fantasma					
Fraude: Tipo/ Esquema	Oportunidad de control	Escenario de fraude	Ocultación	Banderas rojas	Conversión
Malversación/ Empleado fantasma/ Ficticio	Supervisor; pago, recursos humanos	Contratación vía remota permite al supervisor sobrepasar a recursos humanos. Colusión entre el supervisor y la nómina.	Documentos de ID falsos. Registro de tiempo falso. No existe registro de personal.	Documentos perdidos. Letra similar a la del supervisor. Sin registros de tiempo de personal.	Falsa aprobación de cheques, crear una cuenta de banco falso en nombre del empleado.
Malversación/ Empleado fantasma/Baja	Supervisor; el empleado se vuelve un fantasma inexistente	El supervisor no notifica a recursos humanos que el empleado fue dado de baja.	Registros de tiempo falsos, falso cambio a depósitos directos.	Aprobación de cheques, cambio en el depósito directo, cambio en crear registros de tiempo.	Aprobación falsa de cheques, cambiar número de cuenta de depósito.
Malversación/ Empleado fantasma/No existente	Supervisor y empleado	Colusión entre el supervisor y el empleado no existente.	Registros de tiempo falsos.	Sin lugar físico de trabajo, número telefónico o clave de acceso a computadora.	El empleado no existente recibe el cheque de nómina en una cuenta personal.

Apropiación indebida de activos: Empleado fantasma				
Nombre de la organización				
Matriz de la teoría de fraude y auditoría de fraude				
Unidad de riesgo: Apropiación indebida de activos: Empleado fantasma				
Fraude: Tipo/ Esquema	Estrategia de muestreo	Minería de datos	Procedimiento de auditoría de fraude	Conclusión sobre el fraude
Malversación/ Empleado fantasma/ Ficticio	Minería de datos	Investigar los atributos del empleado ficticio.	Inspección física; examinar documentos de identificación originales.	Documentar el fraude. Conclusión.
Malversación/ Empleado fantasma/Baja	Minería de datos	Números de banco duplicados. Identificar empleados dados de baja. Investigar los cambios.	Comparar el registro de tiempo del personal con la agenda de trabajo.	Documentar el fraude. Conclusión.
Malversación/ Empleado fantasma/No existente	Muestreo en bloque por un tiempo	Ninguno.	Determine la evidencia del desempeño de trabajo.	Documentar el fraude. Conclusión.

1.5.5 Teoría del control de fraude

Un elemento central de la teoría del control del fraude está relacionado con la competencia, es interesante saber que la gerencia es responsable por la prevención de fraudes y con mayor probabilidad de recibir entrenamiento relacionado con el fraude y los controles internos. Para alcanzar el nivel de competencia, la gerencia necesita estar entrenada en la teoría fundamental de fraude y estrategias de prevención.

Los inhibidores de control proveen la ilusión de que el control está operando, sin embargo, el perpetrador está violando el control sin ser detectado. Algunos ejemplos de inhibidores de control son los siguientes:

- El que la gerencia anule los controles es la razón número uno por la que se cometen la mayoría de los fraudes, lo cual consiste en el acto de anular y la inexistencia de supervisión del desempeño en sus responsabilidades de control.
- Colusión de empleados, clientes y proveedores puede ocurrir; de hecho, diversos esquemas de fraude requieren colusión. El acto de corrupción es un ejemplo, ya que los perpetradores no se corrompen a sí mismos solamente.
- La aplicación o falta de comprensión de los controles internos conlleva a una negación del valor de la aplicación de los mismos.
- Falsificar documentos que encubren un fraude.

1.5.6 Programas antifraude

La mejor práctica para la prevención del fraude es una organización que cuenta con un programa visible y efectivo antifraude, el programa puede ser relacionado con el modelo de control usado por la organización; al usar el marco COSO por ejemplo, los componentes del programa antifraude serían:

1. **Realizar una evaluación de riesgo de fraude.** Esto consiste en asegurar que la gerencia comprende dónde la organización es vulnerable al riesgo de fraude. La gerencia es claramente responsable por la efectividad completa de la evaluación del riesgo de fraude.
2. **Crear un ambiente de control adverso al fraude.** El ambiente de control debe contar con un adecuado tono en la dirección, el ambiente de control, “soft control” o controles blandos, tienen gran influencia en la efectividad de los procesos de control. Los empleados comprenden rápidamente qué controles internos son importantes para la gerencia y cuáles reciben menos atención de la gerencia. Es por esto que el ambiente de control debería:
 - a) Crear y mantener una cultura de honestidad y normas éticas de negocio.
 - b) Proveer disciplina por violaciones al código de conducta.
 - c) Comunicar el tono apropiado sin tolerancia para las actividades fraudulentas.
 - d) Establecer procedimientos y políticas para prevenir, detectar y detener el fraude.
 - e) Establecer una política asertiva relacionada con la auditoría y la investigación de fraude.
3. **Diseñar e implementar actividades de control antifraude.** Los procedimientos de control interno deben ser relacionados con los riesgos de fraude identificados en la evaluación de los mismos; el objetivo es mitigar los riesgos de fraude consistentes con los objetivos de la gerencia y enfocado en minimizar el fraude a un nivel aceptable. Los controles se refieren tanto a preventivos como detectivos, y el sistema de éstos debe considerar gestionar los inhibidores de control, los cuales anulan las actividades de control.
4. **Compartir información y comunicación.** El código de conducta de la compañía y la política de respuesta al fraude que da la organización, son las claves para comunicar la actitud de no tolerancia hacia estas conductas antiéticas. La posición de la compañía debe ser comunicada periódicamente por medio de libros,



mensajes en línea y entrenamiento, así como por mensajes de la gerencia. Estar alerta al fraude es un aspecto importante del programa antifraude.

5. **Monitorear actividades.** Un componente principal de un programa antifraude es incrementar la percepción de la detección de actividades fraudulentas; los sistemas de monitoreo de fraude y los reportes son herramientas efectivas para alcanzar los objetivos. Los sistemas deben construirse alrededor de los esquemas de fraude identificado en la evaluación de riesgo. Un segundo aspecto del programa consiste en un programa creíble antifraude que se convierta en un detractor para los individuos que han contemplado cometer actos fraudulentos.
6. **Responder a las actividades fraudulentas.** Cuando las denuncias de fraude ocurren, la gerencia necesita tener la habilidad de responder a éstas; asimismo, el uso de una política de respuesta al fraude es la piedra angular del programa. Tanto el uso de auditoría interna y externa como los consultores especializados, son críticos para alcanzar la efectividad del programa.

1.5.7 Importancia del control interno

De acuerdo con el modelo COSO, los procedimientos de control son un elemento para mitigar el riesgo. Un marco de control es una herramienta efectiva de control para documentar los procedimientos de control de fraude. El proceso comienza con la identificación del riesgo de fraude y la relación con la prevención, detección y la disuasión del riesgo de fraude.

Un control preventivo está diseñado para minimizar la probabilidad del riesgo de fraude que ocurre en un sistema de fraude. Las actividades de control marcadas en el modelo COSO proveen una visión completa y autorizada de los procedimientos de control.

Los controles detectivos están diseñados para alertar a la gerencia de que un riesgo de fraude ha ocurrido en un tiempo determinado. Los componentes de monitoreo, supervisión e información del marco COSO proveen procedimientos para la detección de fraude.

Los controles de monitoreo apropiadamente diseñados pueden actuar como un control de detección y disuasión. Los auditores utilizan la teoría de las banderas rojas para identificar el fraude. Lógicamente, la gerencia puede usar la misma teoría del fraude para incrementar su habilidad para monitorear las transacciones de negocio.

En muchos sistemas, un reporte de transacción enlista todos los cambios que han sido revisados; un gerente inicia el reporte de monitoreo indicando la revisión y aprobación. El problema con el reporte es el volumen de cambios y la revisión superficial realizada por muchos gerentes.

Los controles de monitoreo se construyen alrededor de un esquema de fraude; la función es la disuasión por medio de hacer que los esquemas de fraude sean visibles. Los reportes de monitoreo no deben mantenerse en secreto; los empleados deberían ser informados de los resultados, esto con el fin de disminuir la exposición a una colusión lógica.

Los controles de disuasión son diseñados para desmotivar a los individuos de cometer un fraude. La sección de ambiente de control del modelo COSO crea un ambiente para la detección de fraude.

1.5.8 Reporte de auditoría forense

El resultado final de una auditoría de fraude es un documento que provee a las partes de información para tomar las decisiones necesarias. La gerencia necesita saber cuánta evidencia existe para sustentar la investigación. El investigador de fraude y consejo legal necesita entender qué hechos han sido utilizados para soportar las denuncias. El reporte de auditoría forense debe proveer la base para una acción y marco para la investigación. Un reporte de auditoría de fraude escrito en el formato de un experto provee el medio para lograr los objetivos de la auditoría y eventualmente los objetivos legales futuros.

Una transacción sospechosa es aquella que contiene indicadores de fraude, consistentes con el perfil de datos de fraude y el auditor no es capaz de concluir la propiedad de la transacción. Como resultado, el auditor recomienda

una investigación para la obtención de evidencia adicional para soportar las sospechas del auditor y remisión de la autoridad judicial.

El reporte de auditoría forense es una herramienta para documentar y comunicar las sospechas del auditor; las normas de auditoría proveen una guía para que los auditores comprendan su responsabilidad para comunicar problemas, pero no el formato, estilo y contenido requerido. Las normas federales de evidencia proveen un modelo para desarrollar la estructura de un reporte de auditoría forense.

1.5.9 Diferencia entre auditoría forense e investigación de fraude

La manera de responder al riesgo de fraude consiste en comprender la diferencia entre auditoría e investigación, diseñar políticas adecuadas para responder a este riesgo y, por último, proveer de un marco para preparar un plan de investigación.

Comprender la diferencia entre la profesión de auditoría y la investigación es relevante; los auditores e investigadores son diferentes, ellos tienen distintos conocimientos y normas. Los auditores se basan en las normas de auditoría, principios contables, políticas y procedimientos.

Los investigadores se basan en reglas de evidencia y procedimientos criminales o civiles; para un procedimiento criminal, la violación es materia legal y requiere un cuerpo de pruebas; en las acciones civiles, el problema relaciona con los derechos y obligaciones de un contrato que resultan en un posible agravio.

La auditoría de fraude tiene como función identificar transacciones que tienen potenciales banderas rojas de un esquema de fraude, la gerencia se convierte en el juez del hecho porque la investigación de fraude está destinada a refutar o sustanciar la acusación y proveer evidencia relacionada con los activos requeridos de una ley; en donde el juez y el jurado se convierten en quienes juzgarán la verdad del hecho.

Una de las principales preguntas de los auditores que realizan una investigación es:

¿Cuál es el objetivo de la investigación? En general, el objetivo es resolver la acusación o sospecha de fraude; sin embargo, comprendiendo el punto final del caso, los auditores pueden hacer un mejor plan para realizar el de investigación. Los auditores deberían tratar cada caso como si fuera ser llevado a la corte criminal; en este caso, deberán seguir estrictamente los procedimientos y conducta durante la investigación. Debido a la realidad de cómo las organizaciones reaccionan a las acusaciones de fraude; perseguir la acusación con una total extensión no es siempre posible; la auditoría de fraude debe proveer una transición visible de la auditoría a la investigación. Idealmente, el reporte de auditoría forense debe convertirse en el reporte de investigación de fraude con un mínimo de cambios; los puntos principales y finales de la investigación son:

1. Persecución criminal.
2. Restitución civil.
3. Resolución administrativa.
4. Personas claramente inocentes o sospechosas.
5. Mejora del control interno.

1.1 ¿Qué es la auditoría forense?

Preguntas de opción múltiple

1. ¿Cuál de las siguientes es una herramienta eficaz para descubrir actividades en contra de la ética en una organización?
 - a) Selección de solicitantes.
 - b) Entrevista ética.
 - c) Revisión de antecedentes.
 - d) Cuestionario de ética.
2. Las banderas rojas son condiciones que indican una mayor probabilidad de ocurrencia de un fraude. ¿Cuál de las siguientes no es considerada una bandera roja?
 - a) La administración ha delegado la autoridad por realizar compras bajo cierto valor a sus subordinados.
 - b) Un individuo ha mantenido el mismo trabajo de manejo de efectivo por un periodo extendido sin ninguna rotación de actividades.
 - c) Un individuo que maneja bienes comerciales es responsable por realizar las compras, registrarlas y reportar cualquier discrepancia a la alta dirección.
 - d) La asignación de responsabilidad y obligación del departamento de cuentas por cobrar no es clara.
3. ¿Cuál de las siguientes no sería considerada una condición que indique una mayor probabilidad de fraude?
 - a) La gerencia ha delegado la autoridad de hacer compras hasta cierta cantidad límite a los subordinados.
 - b) Un individuo ha mantenido el mismo trabajo de manejo de efectivo por un periodo prolongado, sin ninguna rotación de deberes.
 - c) Un individuo que maneja títulos valores negociables es responsable de hacer las compras, registrarlas y reportar cualquier discrepancia y ganancias y pérdidas a la alta gerencia.
 - d) Las responsabilidades y rendición de cuentas en el departamento de cuentas por cobrar no están claras.
4. Una organización debe tener el debido cuidado de no delegar autoridad discrecional de manera sustancial a personas de la organización que se sabe tienen propensión a participar en actividades ilegales. ¿Cuál de las siguientes opciones son medidas que puede tomar una organización para asegurar que se detecte a tales personas?
 - I. Seleccionar solicitudes de empleo de todos los niveles e investigar delitos pasados, especialmente condenas dentro de la industria de la compañía.
 - II. Preguntar a los profesionales acerca de su historia de disciplina ante consejos de licencia.
 - III. Realizar revisiones de antecedentes de empleados o reportes de crédito de los solicitantes para asegurar que estén bien económicamente y no sea probable que cometan robo o fraude.
 - a) Sólo I.
 - b) Sólo III.
 - c) Sólo I y II.
 - d) I, II y III.

5. ¿Cuál de las siguientes son formas de castigo para quienes violan un código de conducta de la organización?
 - I. Advertencia.
 - II. Pérdida de pago.
 - III. Suspensión.
 - IV. Terminación.
 - a) Sólo I y II.
 - b) Sólo I, III y IV.
 - c) Sólo I, II y III.
 - d) I, II, III y IV.
6. Es una de las características del fraude que consiste en las situaciones que hacen propensas la comisión de un fraude.
 - a) Oportunidad.
 - b) Racionalización.
 - c) Presión.
 - d) Estilo de vida.
7. ¿Cuál de los siguientes controles si son implementados apropiadamente, podrían disminuir la posibilidad de un fraude?
 - a) Requerir la rotación periódica de compras entre diferentes proveedores.
 - b) Requerir la rotación de deberes entre los tres agentes de compras.
 - c) Requerir que los reportes de recepción sean enviados directamente a cuentas por pagar.
 - d) Requerir que las actualizaciones al registro de inventario perpetuo registradas sean hechas por el departamento de recepción.
8. La motivación más común para el fraude gerencial es la existencia de:
 - a) Vicios tales como el hábito de apostar.
 - b) Insatisfacción laboral.
 - c) Presiones financieras en la organización.
 - d) El reto de cometer el crimen perfecto.
9. ¿Cuál de las siguientes actividades representa una función adecuada departamental del personal, así como una manera de evitar un fraude de nómina?
 - a) Distribución de cheques de pago.
 - b) Autorización de tiempo extra.
 - c) Autorización de adiciones y eliminaciones de la nómina.
 - d) Recolección y retención de cheques de pago no reclamados.
10. El control interno puede proporcionar aseguramiento razonable de que los objetivos de la organización se alcanzarán de manera eficiente y eficaz, un factor que limita la probabilidad de alcanzar los objetivos es:
 - a) Que la responsabilidad primaria del auditor interno sea la detección de fraude.

- b) Que el comité de auditoría esté activo y sea independiente.
 - c) El costo del control interno no debe exceder sus beneficios.
 - d) La administración monitorea el desempeño.
11. Para un auditor forense, un empleado que se niega a tomar vacaciones o licencia por enfermedad debe ser visto como:
- a) A los empleados de alta productividad.
 - b) La indicación de la gestión de la teoría X.
 - c) La indicación de la falta de personal en esa área funcional.
 - d) Una bandera roja de un posible fraude.
12. ¿Cuál de las siguientes afirmaciones sobre la detección de violaciones de integridad es la menos precisa?
- a) Las líneas directas de fraude son una buena manera de detectar el fraude, aunque pasiva y correctivamente.
 - b) Los conteos de inventario no anunciados podrían disminuir los robos.
 - c) El cambio frecuente y regular de contraseñas ayuda a prevenir el acceso no autorizado al sistema.
 - d) Asegurar que los funcionarios que realizan contrataciones hagan una declaración anual de su conocimiento de las leyes y reglamentos pertinentes para realizar este procedimiento, esto disminuirá el fraude de adquisiciones.
13. Un sistema adecuado de controles internos puede detectar con más probabilidad un fraude realizado por:
- a) Un grupo de empleados coludidos.
 - b) Un solo empleado.
 - c) Un grupo de administradores coludidos.
 - d) Un administrador.
14. Un fraude es detectado con mayor frecuencia por medio de:
- a) E-mails.
 - b) Denuncias.
 - c) Auditoría interna.
 - d) Análisis de la dirección.

1.2 Nuevas formas de fraude y sus características

Autoevaluación de vulnerabilidad ante el cibercrimen

Por medio de estas preguntas se puede realizar un diagnóstico sobre la vulnerabilidad de la empresa o entidad pública ante el cibercrimen.

Autoevaluación organizacional

1. ¿Qué alertas de la existencia de delitos cibernéticos presenta su empresa?
2. En su compañía, ¿existe una apropiada capacitación para identificar los delitos cibernéticos?

3. ¿Se tiene un equipo con experiencia en la respuesta a incidentes relacionados con los delitos cibernéticos?
4. ¿Su organización ha experimentado un delito cibernético? ¿Qué medidas han tomado para prevenirlo?
5. ¿Existe un proceso documentado acerca de cómo actuar en caso de detectar un delito cibernético?
6. ¿La organización conoce el marco legal que la protege de la ciberdelincuencia, así como las organizaciones a las que puede acudir en caso de ser víctima?

Autoevaluación de vulnerabilidad al cibercrimen individual

1. ¿Con qué frecuencia existen diferencias en pesos y centavos en las cuentas bancarias que aparentemente son irrelevantes?
2. ¿Ha ingresado su usuario y contraseña en su computadora, correo electrónico o cajero automático y ha tenido que repetir la operación dos o tres veces porque el sistema le dice que sus datos no corresponden?
3. ¿Cuántas veces le ha dado su información vía telefónica a un supuesto empleado bancario?
4. ¿Cuántas veces ha respondido a un supuesto aviso bancario donde le piden datos personales como usuario y contraseña?
5. ¿Con qué periodicidad actualiza el antivirus de la computadora donde realiza sus transacciones por medio de Internet?

1.3 Comprensión y análisis del fraude ocupacional

Análisis de video

Conteste las preguntas de análisis después de visualizar el siguiente video:

Fraudes Financieros Caso Enron
<https://www.youtube.com/watch?v=108AGkqp5J8>
ENRON. Los chicos más brillantes del salón

1. ¿Cuáles son las preguntas que realiza el juez y que la auditoría forense deberá responder?
2. ¿Cuáles son los factores internos y externos que permitieron el fraude en la empresa Enron?
3. ¿Cuáles son los indicios de fraude en la organización y en la alta dirección que se mencionan en el video?
4. ¿Cuáles son las características de la cultura de Enron?
5. ¿Qué tipo de fraudes y debilidades de control ocurrieron en la empresa Enron?



1.4 Prevención, disuasión y detección de fraude

Índice de madurez para la prevención y detección de fraude en la organización

Los siguientes enunciados representan prácticas y controles que las organizaciones deben adoptar para contar con un programa de prevención y detección de fraude apropiada; marque la casilla con el número que mejor identifique a su organización en donde el 1 representa el menor cumplimiento del enunciado y el 5 el mayor. Posteriormente, sume la puntuación total y calcule el índice de madurez para la prevención y detección de fraude de su organización como se indica.

1. Todos los puestos cuentan con una descripción de puesto escrita.

1	2	3	4	5
---	---	---	---	---

2. Existe y se aplica un manual organizacional que muestra las líneas de responsabilidad y comunicación.

1	2	3	4	5
---	---	---	---	---

3. Existen políticas relacionadas con la contabilidad y finanzas y, de igual manera, especifican quién tiene responsabilidad y autoridad sobre las transacciones.

1	2	3	4	5
---	---	---	---	---

4. Existe en la organización un código de ética y se implementa, los empleados conocen qué conductas se esperan de ellos; asimismo, la alta dirección da el ejemplo de su cumplimiento y una persona de alta jerarquía es encargada de vigilar su cumplimiento.

1	2	3	4	5
---	---	---	---	---

5. Existe un programa antifraude en la organización, que incluye políticas antifraude escritas, capacitación para los empleados acerca del tema, una persona encargada del cumplimiento de la política y medios formales para comunicar sospechas de fraude.

1	2	3	4	5
---	---	---	---	---

6. La organización cuenta con mecanismos para la recepción de denuncias de posibles fraudes, un registro de todos los casos e investiga estas sospechas de manera inmediata y exhaustiva.

1	2	3	4	5
---	---	---	---	---

7. La organización realiza labores de prevención del fraude como la revisión de antecedentes de empleados, existe una función de prevención de pérdidas, auditoría interna y personas encargadas del cuidado de los activos.

1	2	3	4	5
---	---	---	---	---

8. El clima de la organización favorece el clima ético. Que los empleados se sientan tratados y recompensados de manera justa, mantiene una comunicación adecuada con sus superiores, la rotación de personal es baja, el desempeño se mide de forma justa y realista.

1	2	3	4	5
---	---	---	---	---

9. Los empleados mantienen una conducta adecuada, que no incluye señales de alerta como estilo de vida que excede lo que percibe, adicción al alcohol o juegos de azar, intereses fuera de la organización que son incompatibles con su puesto.

1	2	3	4	5
---	---	---	---	---

10. La organización cuenta con un sistema de controles de acceso a información sensible, así como contraseñas sólo para personal autorizado, utiliza la tecnología para monitorear accesos a información por personal no autorizado.

1	2	3	4	5
---	---	---	---	---

11. La organización utiliza técnicas como el monitoreo continuo de datos, análisis de ratios, revisiones sorpresa de inventarios, arqueos de efectivo, confirmaciones con el banco, análisis estadísticos, entre otras, que le permiten detectar y prevenir la existencia de fraude.

1	2	3	4	5
---	---	---	---	---

12. Existe una adecuada segregación de funciones del personal, así como supervisión continua y rotación de funciones en puestos clave o de alto riesgo.

1	2	3	4	5
---	---	---	---	---

13. Existe un área de compras de la organización que es independiente del de contabilidad, recibo y envío, esta área es supervisada por la gerencia de quien recibe autorización para la aprobación de las compras; existen políticas de compras relacionadas con montos, cantidades, precios y días, así como formatos para realizar una orden; existe un proceso de compra coordinado con otras áreas que permite detectar inconsistencias.

1	2	3	4	5
---	---	---	---	---

14. La nómina es una función que se mantiene separada de otras áreas, cuenta con registros que se generan de manera independiente acerca de los empleados y las incidencias que afectan los pagos, mantiene una lista actualizada de personal que labora con salarios en montos correctos. Existe un supervisor que verifica y firma las tarjetas de tiempo del personal.

1	2	3	4	5
---	---	---	---	---

15. Existe una política acerca de recibir o dar regalos a los clientes o proveedores en la organización, existen políticas anticorrupción, se verifican los posibles conflictos de interés existentes, las políticas de licitación se cumplen y respeta el debido proceso, existe tolerancia cero en la organización a actos de corrupción.

1	2	3	4	5
---	---	---	---	---

16. Puntuación obtenida: _____ / 75 (Puntuación total) × 100

Índice de madurez de la organización en la prevención y detección de fraude = _____%

Nota: A mayor porcentaje obtenido, mayor madurez en la organización.

1.5 Control interno para prevenir el fraude

Formatos para realizar una evaluación de riesgos y controles

Paso 1: Identificación de controles

Control	Persona responsable del control	Procedimiento para ejecutarlo	Justificación de su existencia	Periodicidad con que se ejecuta	Cuando el control se considera terminado	Producto o salidas del control
#1 Ej. Bitácora de inventario entrante	Responsable de recepción	El responsable realiza un conteo de la mercancía entrante y lo registra en la bitácora de inventario.	Este control permite conocer las existencias de mercancía y necesidades de compra.	Cada vez que ingresa mercancía al área de recepción.	Cuando el encargado de bodega realiza nuevamente el conteo y verifica dando su Vo. Bo.	Registro de inventario entrante.
#2						
#3						
#4						
#5						

Paso 2: Elaboración de diagrama de flujo y narrativa

Diagrama de flujo y narrativa			
Proyecto:	Fecha:	Objetivo:	
Nombre del proceso:	Nombre del subproceso:		
Entrada	Proceso	Salida	Narrativa
<pre> graph LR Start([Entrada]) --> A[] A --> B[] B --> C{ } C --> D[] D --> E[] E --> F[] F --> End([Salida]) </pre>			Ej. De manera semanal, el encargado de recursos humanos actualiza la lista de personal con base en la información soporte.
Validado por:	Situación actual:	Firma y/o código:	

Paso 3: Matriz de funciones y responsabilidades

Matriz de funciones y responsabilidades								
Nombre de la entidad								
Nombre del puesto								
Departamento								
Nombre de la persona								
Descripción detallada	Descripción detallada de funciones y responsabilidades	Elabora	Revisa/autoriza	Registra	Características de reportes principales	Registro contable		
						Cuenta	Débito	Crédito

Observaciones:

Elaborado por		Fecha	
Elaborado por		Fecha	

Paso 4: Matriz de riesgos y controles

Matriz de análisis de riesgos y controles														
Referencia de control	Objetivo de control	Actividad de control	Anomalía	Clasificación del control				Evaluación del control				Alcance de aplicación		
				Manual	Automático	Proactivo	Detectivo	Totalidad	Exactitud	Validez	Acceso restringido	Organización	Área	Proceso

**Paso 5: Ejecución y documentación de recorridos**

Ejecución y documentación de recorridos			
Nombre de la entidad			
Código de proceso			
Proceso			
Subproceso			
Dueño del proceso			
Referencia al flujograma	Descripción detallada de las actividades recorridas	Observaciones y/o comentarios	Referencia soporte
Observaciones:			
Elaborado por		Fecha	
Elaborado por		Fecha	

Paso 6: Elaboración de plan de pruebas

Plan de pruebas						
Prueba	Tipo de prueba		Periodo de prueba	Técnicas de evaluación	Tamaño de la muestra	Criterios de evaluación
	Manual	Automática				

Paso 7: Reporte de deficiencias

Reporte de deficiencias							
#	Dimensión	Proceso crítico	Área de oportunidad	Riesgos	Recomendación/ Plan de acción	Prioridad	Referencia
Ej. 12	Procesos	Administración	No existe un procedimiento formal de detección de fraude.	Escenario que facilita la existencia de fraude.	Implementar mecanismo de detección de fraude relacionado con el control interno.	Alta	D

Paso 8: Plan de remediación

Plan de remediación					
Deficiencia	Actividad de remediación	Impacto esperado	Nivel de esfuerzo requerido	Responsable de implementación	Tiempo requerido



Respuestas de ejercicios

ANEXO 1.1

Clave: 1a, 2a, 3a, 4c, 5d, 6a, 7c, 8c, 9c, 10c, 11c, 12d, 13d, 14a.

ANEXO 1.3

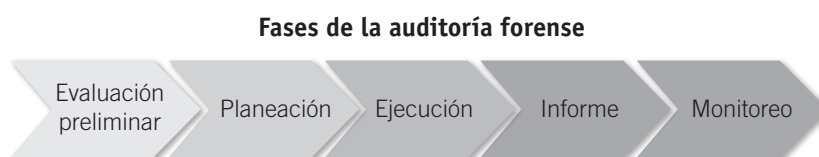
1. ¿Cuáles son las preguntas que realiza el juez y que la auditoría forense deberá responder?
¿Qué sucedió?, ¿quién es responsable?, y ¿qué podemos hacer para prevenir este tipo de problemas en el futuro?
2. ¿Cuáles son los factores internos y externos que hicieron propensa a la empresa Enron al fraude?
Crecimiento acelerado de 10 a 69 billones de dólares en activos.
Falta de gobierno corporativo y supervisión de las operaciones clave, adquisiciones y estrategia.
3. ¿Cuáles son los indicios de fraude en la organización y en la alta dirección que se mencionan?
Características organizacionales como el orgullo, arrogancia, intolerancia, avaricia.
Destrucción de papeles.
Venta de acciones de manera rápida por miembros de la alta dirección.
Falta de respeto de los directivos hacia las normas y regulaciones del gobierno.
Valores morales que no respaldan la toma de decisiones.
Cuentas de banco clandestinas.
Contabilidad alterada.
Estaba involucrada con la política.
Crecimiento acelerado.
Tráfico de influencias y compras fraudulentas.
4. ¿Cuáles son las características de la cultura de Enron?
Cultura de sobrevivencia del más fuerte.
Alcanzar los objetivos sin importar cómo.
Alto apetito de riesgo.
Cultura machista.
5. ¿Qué tipo de fraude y debilidades de control se dieron en la empresa Enron?
Se detectó fraude en tarjetas y manejo de fondos debido a que tenían un buen desempeño.
Informes financieros fraudulentos.
Falta de investigación en inversiones y adquisiciones.
Fraude ocupacional y en los estados financieros.

Metodología de auditoría forense

2.1 Metodología de auditoría forense

La auditoría forense puede dividirse en cinco fases, durante cada una de ellas se realizan actividades específicas; este esquema de auditoría se propone utilizar para las auditorías forenses preventivas y detectivas, mismas que podrían incluirse dentro del plan anual de auditorías de la organización.

Ilustración 22. Fases de la auditoría forense



Fuente: Elaborado por el autor.

2.1.1 Evaluación preliminar

La primera fase es la evaluación preliminar y de riesgos de la empresa, que consiste en evaluar el entorno en el que se encuentra la organización, por ejemplo y, de manera amplia, el auditor deberá conocer el objeto social de la empresa, clientes potenciales, competencia, acreedores, relaciones financieras, misión, visión, objetivos, planes o metas, entre otros; generando así un expediente documental de antecedentes y situación financiera, mismo que puede contener lo siguiente:

- Copia de estatutos: constitución y reformas.
- Certificado de existencia y representación legal.
- Copia de permisos de funcionamiento y licencias.
- Situación legal en todos los órdenes.
- Partes interesadas.
- Operaciones actuales.
- Planeación estratégica.
- Estructura para afrontar la globalización.
- Contratos a largo plazo.
- Estudios actuariales.
- Garantías otorgadas.
- Títulos de propiedad y sus gravámenes.
- Convenios y/o pactos colectivos de trabajo.

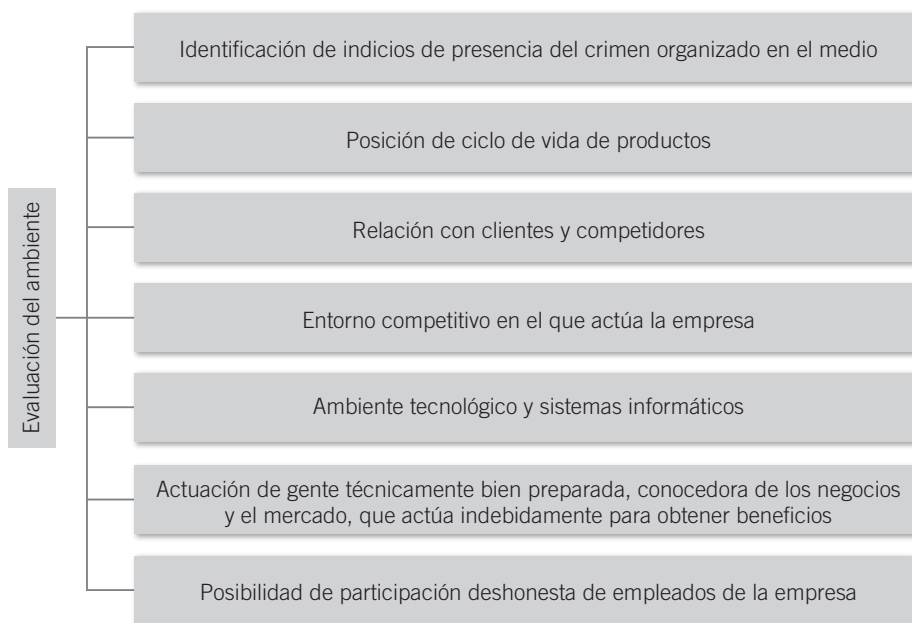
- Contratos o convenios especiales.
- Normatividad y legislación aplicable.
- Estados financieros (últimos cinco años).
- Indicadores financieros: EBITDA, EVA, TIR, BAI, BDI, entre otros.
- Indicadores de industria.
- Análisis de viabilidad como empresa en marcha.
- Determinación del punto de equilibrio.
- Sistema de información financiera y contable, software de contabilidad utilizado.
- Calidad de la operación, personal y organización del departamento de contabilidad.
- Estado de los libros de contabilidad.
- Indicadores de riesgo/mapa de riesgo general.
- Informes y dictámenes de revisión fiscal (cinco años).
- Informes de gestión (cinco años).
- Expediente de recursos humanos.
- Método de selección de personal.

Esta información debe ser del conocimiento del equipo encargado de realizar auditorías forenses, así como de los auditores internos en su caso; se considera que la comprensión y conocimiento de esta información permitirá estar alerta y analizar posibles esquemas de fraude, malversación y otros actos tipificados como fraude. Asimismo, permitirá al auditor forense actuar respecto de las características específicas de la organización auditada.

Para el auditor forense en específico, es primordial conocer las leyes, normas, regulaciones nacionales e internacionales, debido a que cualquier violación de éstas deberá ser reportada e identificada como parte de la auditoría forense.

Durante la evaluación preliminar, el auditor forense deberá hacer mayor énfasis en la evaluación del ambiente de la organización, conformado por los siguientes factores:

Ilustración 23. Evaluación del ambiente interno de fraude

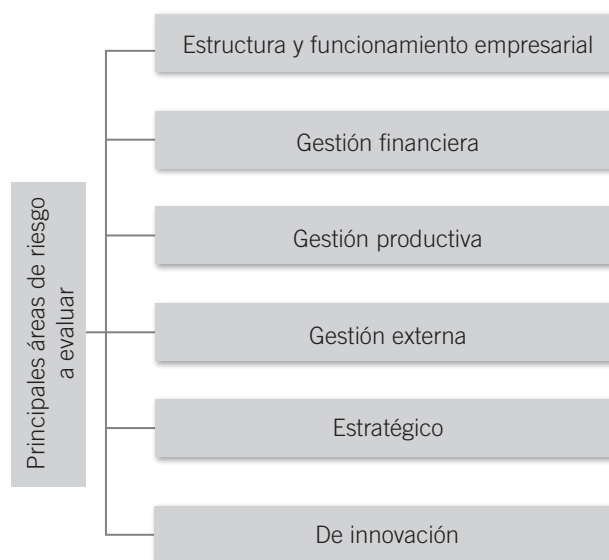


Fuente: Elaborado por el autor.

La evaluación de riesgos de fraude forma parte del proceso de gestión de riesgos general de la organización. Por tal motivo, el auditor forense debe familiarizarse en esta etapa con tal proceso y evaluar si se están aplicando controles adecuados y relevantes a los riesgos relacionados con el fraude.

Existen áreas especialmente importantes en la evaluación preliminar que el auditor deberá comprender en cuanto a su funcionamiento y Sistema de Gestión de Riesgos y Control.

Ilustración 24. Principales áreas de riesgo de fraude



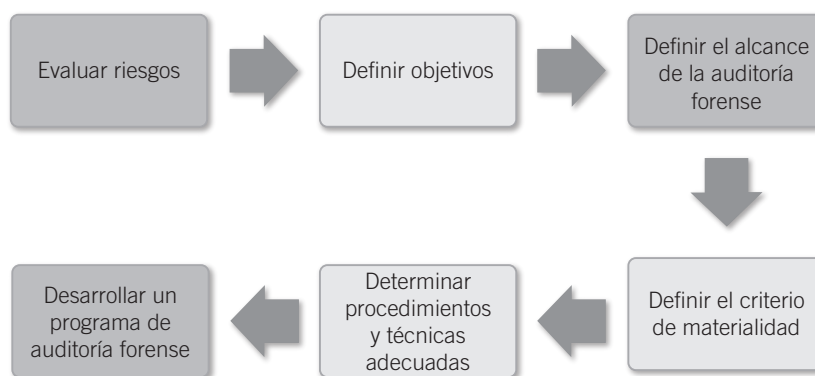
Fuente: Elaborado por el autor.

Evaluando las principales áreas de riesgo, el auditor puede tener un marco de referencia e identificar las transacciones que deben ser objeto de una auditoría forense, esto puede provenir de un catálogo de tipos de transacciones susceptibles de ser investigadas o por muestreo a transacciones que se tipifican.

2.1.2 Planeación

Las Normas Internacionales de Auditoría (NIA), en específico la norma 300, señala que cualquier trabajo de auditoría debe ser técnicamente planeado para alcanzar los objetivos trazados en la forma más eficiente posible. La planeación de la auditoría forense deberá incluir, por lo menos, los siguientes pasos:

Ilustración 25. Proceso de planeación de la auditoría forense



Fuente: Elaborado por el autor.

Evaluación de riesgo de fraude

El auditor forense debe conocer la efectividad con el cual el proceso opera y las observaciones que hayan surgido de auditorías previas para enfocar la auditoría forense a las áreas con mayor riesgo.

El riesgo de fraude está asociado con áreas y transacciones con mayor propensión al mismo, debido a una falta de controles o a la naturaleza de los activos que administran; durante la planeación, el auditor forense realiza una priorización de estos riesgos de lo general a lo específico, mediante procedimientos diversos como revisión de auditorías internas y externas anteriores, reportes del sistema de evaluación de riesgos, reportes generados por diversas áreas de la organización, naturaleza del trabajo de áreas o puestos, así como procedimientos analíticos realizados para diversas cuentas, transacciones u operaciones y banderas rojas observadas.

Toda la información recabada debe ser clasificada y priorizada para identificar las áreas de mayor riesgo de fraude que se incluirán en la planeación.

Definición de objetivos

Una vez identificadas las áreas, transacciones, sucursales y personas que serán sujetos a revisión, deberán definirse claramente los objetivos de la auditoría forense; éstos definirán la naturaleza de los procedimientos a aplicar, así como el alcance e información necesaria que se requerirá obtener durante la ejecución.

Los objetivos deben ser claros y precisos; deben formularse como preguntas o hipótesis a probar en los que el auditor debe tener cuidado de no incluir términos ambiguos, abstractos o desenfocados, así como debe permitir identificar los elementos específicos de los hallazgos necesarios para cumplir con el objetivo.

Definir el alcance de la auditoría forense

El alcance de la auditoría es la extensión de las áreas que serán sujetas de revisión de acuerdo con el objetivo planteado; para definir el alcance se deberá tomar en cuenta el periodo que será cubierto por las pruebas de auditoría, la información que está disponible para su realización, así como la evidencia necesaria para probar algún posible delito en caso de que se detectara.

El alcance de auditoría podrá establecerse durante la planeación, pero como se mencionó con anterioridad, la auditoría forense mantiene un enfoque flexible, en donde en caso de ser necesario podrá ampliar el alcance de las pruebas realizadas para obtener mayor información.

Es importante contar con el respaldo del consejo de administración durante el establecimiento del alcance de auditoría forense, ya que se requerirá autoridad para acceder a registros, personal y bienes relevantes con alta probabilidad de detección de fraude.

Definir el criterio de materialidad

Durante la planeación, el auditor forense debe identificar cuáles son los parámetros que la organización ha establecido como diferencias o inconsistencias materiales, de tal modo que durante la obtención de la información obtenga datos que sean suficientes y relevantes para probar o desechar la hipótesis de la existencia de algún fraude.

Asimismo, establecer la materialidad permite realizar una auditoría rentable en términos de costo/beneficio y enfocarse en los fraudes que pudieran estarse cometiendo sobre cuentas o activos importantes y de mayor impacto económico.

Determinar procedimientos y técnicas adecuadas

Las técnicas y procedimientos son las que diferencian a la auditoría forense de otros tipos de auditoría; durante la planeación y de acuerdo con la naturaleza y objetivo del trabajo, el auditor define qué procedimientos y técnicas se aplicarán; éstas pueden ser cuantitativas (procedimientos analíticos, estadísticos, comparativos o cálculos) o cualitativas (pruebas de controles, entrevistas, fotografías o grabaciones).

Existe un amplio número y tipos de técnicas existentes de auditoría forense, mismas que tienen que ser altamente confiables debido a que en caso de que se detectara la existencia de fraude, ésta puede utilizarse en un futuro caso de litigio ante instancias judiciales.

Desarrollar un programa de auditoría forense

El programa de auditoría forense debe incluir objetivos, resultados de análisis de riesgos del área a auditar, técnicas y procedimientos, así como tiempos y consideraciones especiales del cuidado de la información y cadena de custodia. El programa de auditoría forense debe estar acompañado de un protocolo de acciones que deberán tomarse en caso de detectar algún tipo de fraude y líneas de comunicación con el consejo y la alta dirección.

2.1.3 Ejecución

La ejecución es la parte central de la auditoría forense y la que la diferencia de otros tipos de auditoría, y consiste en los siguientes pasos:

Ilustración 26. Ejecución de auditoría forense



Fuente: Elaborado por el autor.

Recopilación de evidencia por medio de procedimientos y técnicas

El primer paso de la ejecución es la recopilación de información por medio de procedimientos y técnicas de auditoría forense especializadas; por lo general, éstas se realizan mediante análisis computarizados; la evidencia debe estar relacionada con el objetivo de la auditoría y cumplir con requisitos mínimos de calidad, ya que en una auditoría forense se presume la alta probabilidad de un fraude y, por ende, una posterior instancia legal-judicial a la que deberán presentarse las evidencias recabadas.

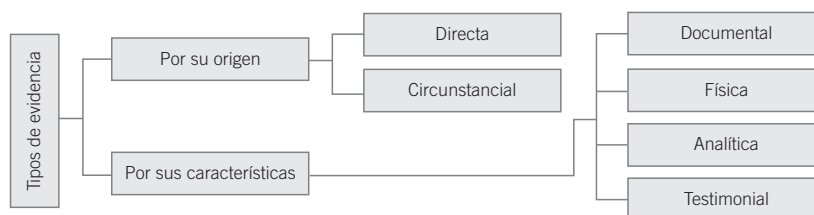
Respecto a la evidencia, la NIA 500 menciona que la evidencia sirve al auditor para llegar a conclusiones razonables en las cuales basar su opinión por medio de un análisis y revisión para determinar la consistencia y confiabilidad de los registros contables, hechos y cifras.

Existen diferencias importantes entre la evidencia y la prueba en términos legales; así, la evidencia es cualquier objeto relacionado con una conducta que sirve para determinar las circunstancias reales de tiempo, modo y lugar en las que el hecho se realizó y que deberá someterse al régimen de cadena de custodia. Mientras la prueba es considerada como aquel elemento que, una vez se hace parte de un proceso judicial, pretende hacer llegar al convencimiento acerca de la certeza de la existencia u ocurrencia de un determinado hecho.

Es importante que el auditor forense durante la aplicación de los procedimientos para la obtención de evidencia considere que ésta podría convertirse en prueba para un futuro proceso judicial, en la que deberá ser lo suficientemente convincente para establecer la responsabilidad de un acusado como autor del fraude o partícipe del mismo.

El auditor forense, mediante técnicas diversas, obtiene evidencia física, documental, analítica o testimonial que puede ser directa o circunstancial, misma que deberá estar relacionada con el objetivo de la auditoría. Éstas se utilizarán como pruebas en un proceso judicial en caso de determinar la existencia de un fraude y el auditor fungirá como perito. Las clasificaciones de la evidencia son:

Ilustración 27. Tipos de evidencia



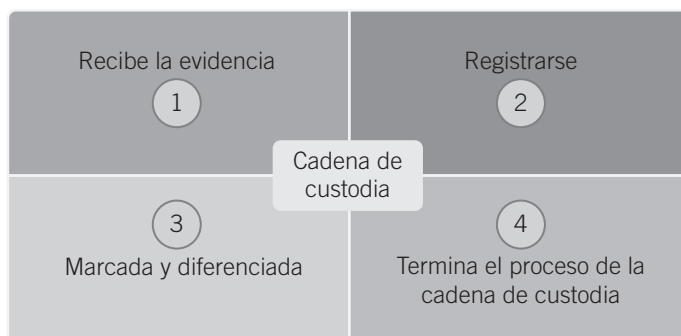
Fuente: Elaborado por el autor.

- a) **La evidencia física.** Se obtiene cuando el auditor realiza una inspección u observación directa de las actividades ejecutadas, de los registros o de hechos.
- b) **La evidencia testimonial.** Es la información obtenida mediante cartas, entrevistas o declaraciones recibidas en respuestas a indagaciones. Estos resultados deben figurar en los papeles de trabajo. Cuando se trata de indagaciones es importante que los resultados de las entrevistas sean firmados por los entrevistados.
- c) **La evidencia documental.** Es la forma más común y consiste en contar con documentos que sustentan los hallazgos y que pueden clasificarse según su procedencia, en externos (se originan fuera de la entidad) e internos (se originan en la entidad misma).
- d) **La evidencia analítica.** Se obtiene al verificar o analizar la información que es suministrada por la entidad por medio de informes o listados computarizados, leyes y reglamentaciones. Lo importante de la evidencia es que se encuentre debidamente sustentada y comprobada; por ello, el auditor deberá registrarlos en los respectivos papeles de trabajo que deben ser elaborados conservando los criterios de orden y legibilidad.
- e) **Evidencia directa.** Es aquella que prueba la existencia del principal o del hecho sin ninguna inferencia o presunción. Se da en el caso de quien tiene conocimiento de los hechos por medio de los sentidos y jura para verificar los hechos en disputa. Puede tomar la forma de admisiones o confesiones hechas en o fuera de la corte (tribunal).
- f) **Evidencia circunstancial.** Es aquella que tiende a probar la existencia del hecho principal mediante la inferencia. Las cortes (tribunales) la reconocen como un medio legítimo de prueba. Incluye probar algunos hechos materiales, mismos que cuando se consideran en sus relaciones con otros, tienden a establecer la existencia del principal o hecho último. En muchos casos es la única disponible cuando se trata de combatir el fraude y el crimen económico.
- g) **Evidencia secundaria.** Es toda aquella que no satisface la mejor regla de evidencia y se le entiende como sustituto de la evidencia documental. Es el caso de las copias de los documentos, si bien puede ser de naturaleza muy variada (fotografías, fotocopias, microfilmaciones, escaneado, transcripciones, gráficas, cronogramas, resúmenes, notas, diarios, papeles de trabajo, memorandos, registros oficiales, etc.). De hecho tiene que tener vinculación directa con el hecho que se pretende probar.

Cadena de custodia

La cadena de custodia es el proceso mediante el cual se identifica y asegura la información durante el proceso de auditoría. El auditor forense debe estar consciente de que debido a la probable existencia de algún fraude, el defraudador u otras partes involucradas pueden intentar alterar o eliminar información relevante para un posible proceso judicial. Por tal motivo, el auditor interno deberá mantener un adecuado cuidado y manejo de información. La cadena de custodia consiste en cuatro pasos:

Ilustración 28. Fases de la cadena de custodia



Fuente: Elaborado por el autor.

La cadena de custodia permite la identificación de todo tipo de evidencia recabada o creada por el auditor, lo cual le da valor para convertirse posteriormente en prueba y asegura su autenticidad e integridad.

A continuación se presenta un formato general como ejemplo, que puede aplicarse a todo tipo de documentación u objetivos físicos que se obtienen durante la auditoría.

Formato de cadena de custodia (datos generales)		
Fecha	Hora	Expediente
Nombre de la autoridad		
No. de teléfono		Unidad/Fiscalía
Nombre de quien embala		
No. de teléfono		Unidad/Coordinación
Domicilio del aseguramiento		
Lugar del aseguramiento y observaciones		

Asimismo, los indicios o elementos contenidos en el formato general deberán ser identificados individualmente, para proteger la información de cualquier daño mínimo que puede hacer la diferencia en un juicio.

Datos particulares del indicio					
Tipo de indicio		Marca		Modelo	
No. de serie		Inventario		Color	
Marcas					
Observaciones					

Evaluación de la evidencia obtenida

La evidencia para ser útil al auditor deberá evaluarse en particular y en su conjunto, asegurándose que cumple con las características de: suficiencia, relevancia, confiabilidad y utilidad.

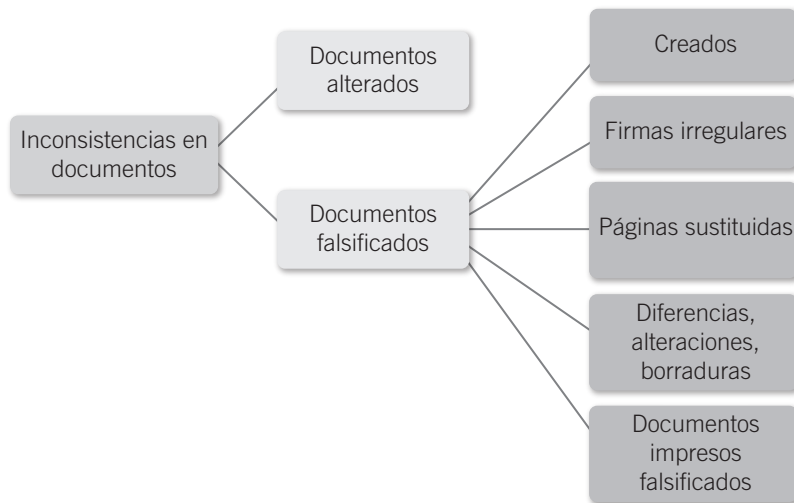
- La evidencia es suficiente cuando está basada en hechos, es adecuada y convincente; de modo que una persona prudente e informada sacaría las mismas conclusiones que el auditor; la suficiencia se evalúa sobre la evidencia como un todo; por ejemplo, ante un juicio en la corte todos los elementos recopilados por el auditor deben ser suficientes para que el juez llegue a las mismas conclusiones que el auditor en relación con el presunto fraude.
- La evidencia es fiable cuando la fuente de la que proviene o las técnicas empleadas para obtenerla son confiables; durante la ejecución de auditoría el auditor debe asegurarse, por ejemplo, así como durante el curso de una entrevista corroborar la información recibida con otros documentos, de manera que el testimonio sea una evidencia fiable. Asimismo, los procedimientos deberán ser aplicados de manera adecuada para lograr que la información obtenida mediante ellos sea considerada fiable o confiable.

Por ejemplo, en relación con la fiabilidad, un documento original es más fiable que una copia; una declaración oral corroborativa es más fiable que una sola declaración; las fotografías son consideradas como una evidencia débil, pero pueden ser corroboradas con un testimonio competente; las fuentes independientes son más fiables dado que las fuentes internas pueden estar involucradas en el fraude, así como la opinión de un experto es de mayor fiabilidad.

- c) La evidencia relevante es la que apoya las observaciones y recomendaciones del trabajo y es compatible con sus objetivos; tiene relación lógica con los hallazgos ejemplo: Una orden de compra que está apropiadamente emitida y aprobada, no es relevante para probar que los bienes ordenados fueron recibidos y que no existe fraude de robo de activos.
- d) La evidencia útil es la que está disponible para la revisión del auditor en el tiempo adecuado y también ayuda al logro de los objetivos de la auditoría.

Adicionalmente, al evaluar la información más que en cualquier otro tipo de auditoría, el auditor forense debe considerar la posible alteración de documentos de otras fuentes de información relevantes, tales como:

Ilustración 29. Inconsistencias en documentos de evidencia



Fuente: Elaborado por el autor.

Ante la posibilidad de participar en un proceso legal, el auditor deberá contar con la mejor información obtenible, por lo que se puede decir en síntesis que requiere información con fortaleza jurídica, cuyas características se presentan a continuación:

Ilustración 30. Evaluación de la evidencia

Evidencia fuerte	Evidencia débil
Objetiva	Subjetiva
Documentos	Opiniones
Opiniones informadas de expertos	Opiniones poco informadas
Directa	Indirecta
De sistemas con buen control interno	De sistemas de control interno débil
Independiente de las operaciones del cliente del trabajo	Preparada por el cliente de trabajo
Toma de muestras estadísticas	Toma de muestras no estadística
Corroborada	No corroborada
A partir de registros preparados en una base oportuna	A partir de registros preparados después de un tiempo.

Fuente: Elaborado por el autor.

Documentación e integración de expediente

La información recabada durante la ejecución de los procedimientos deberá estar adecuadamente documentada en los papeles de trabajo, bajo cadena de custodia y con controles adecuados contra cambios o ataques; el auditor debe asegurarse de que la documentación sea resguardada y de que existan políticas de acceso a la información; sobre todo en una auditoría forense esto cobra mayor relevancia, ya que sólo las personas responsables del trabajo podrán tener acceso y deberá existir un protocolo y línea de comunicación clara acerca de quiénes pueden conocer la información recabada durante la auditoría forense.

2.1.3.1 Procedimientos y técnicas para la obtención de información

Los auditores forenses recurren a diversas técnicas especializadas para la identificación e investigación de presuntos fraudes; los procedimientos y técnicas empleados dependen de la naturaleza de la información que se pretende obtener o anomalías detectadas. Algunos de los procedimientos, técnicas y herramientas se presentan a continuación y se pretende presentarlas desde lo más general hasta lo específico.

2.1.3.2 Procedimiento de cumplimiento

El primer procedimiento que un auditor forense debe realizar es la evaluación de cumplimiento o de control, mismo que proporciona evidencia de que los controles clave existen y de que son aplicados efectiva y uniformemente; aseguran o confirman la comprensión de los sistemas de la organización, particularmente de los controles clave dentro de dichos sistemas, y corroboran su efectividad. Esta evidencia respalda las afirmaciones sobre los componentes de los estados financieros y, en consecuencia, nos permite tomar decisiones para modificar el alcance, naturaleza y oportunidad de las pruebas sustantivas.

- a) **Indagaciones con el personal.** Consiste en obtener información del personal de la entidad en forma oral o escrita, mediante la cual obtengamos evidencia respecto al cumplimiento de algún procedimiento de control interno; la confiabilidad de la información obtenida dependerá en gran medida de la competencia, experiencia y conocimiento de los informantes. Este tipo de información por sí sola no es confiable, sino que requiere que sea corroborada por medio de otros procedimientos.
- b) **Observaciones de determinados controles.** Esta prueba proporciona evidencia en el momento en que el control se realiza y es utilizada para corroborar ciertos tipos de procedimientos de control interno que, por lo general, no se pueden repetir y, por lo tanto, requerimos su observación y comprobación “in situ”, para satisfacernos que los controles observados han operado en forma efectiva.
- c) **Repetición del control.** Generalmente, este procedimiento es utilizado cuando el control no es documentado mediante una firma inicial u otra forma de evidencia y/o cuando requerimos corroborar el cumplimiento de dicho control; así, por ejemplo, si hemos decidido confiar, como control clave, en la revisión de cálculos aritméticos y en la existencia de la documentación de respaldo necesaria para el registro y pago de una transacción, debemos revisar que dicho control funcione eficazmente mediante la repetición del mismo.
- d) **Inspección y revisión de documentos.** Consiste en verificar que los controles clave determinados a efectos de satisfacernos de las afirmaciones para cierto número de cuentas y/o transacciones, se encuentren debidamente respaldados con la documentación de sustento pertinente, ratificando de esta manera que los controles sobre los cuales se decidió confiar inicialmente, operan eficazmente.

2.1.3.3 Procedimientos generales

- Obtener los estados financieros básicos y complementarios, las notas a dichos estados y los registros contables que los respaldan.
- Verificar que los estados financieros estén firmados por las autoridades pertinentes en ejercicio a la fecha de emisión de los mismos (máxima autoridad ejecutiva de la entidad, el responsable del área financiera y el contador general de la entidad) y sustentados con registros contables legalizados oportunamente.

- Efectuar pruebas de consistencia entre los saldos de los estados financieros, estados de cuenta adjuntos, cuadros, anexos y notas.
- Verificar la exactitud aritmética de los registros.
- Verificar la coincidencia de los saldos de los estados financieros con los registros (cuentas del mayor, auxiliares y subcuentas).
- Verificar el tipo de cambio utilizado para los saldos en moneda extranjera.
- Determinar una muestra y efectuar pruebas de apropiación contable y presupuestaria, y verificar que la documentación de sustento sea pertinente y suficiente.
- Conciliar los saldos de la ejecución presupuestaria con el estado de resultados y evaluar la justificación de las diferencias.
- Efectuar la lectura de las actas de director o de los consejos respectivos y contratos importantes, a fin de obtener conocimiento de decisiones significativas que se hayan tomado durante el ejercicio y del cumplimiento de disposiciones legales aplicables que resulten significativas para el logro de los objetivos de la auditoría.
- Obtener información de los hechos subsecuentes que puedan tener efecto significativo sobre los estados financieros y consecuentemente en la opinión. Determinar si existen hechos subsecuentes relevantes que no originen efectos contables, pero que deban ser expuestos en notas a los estados financieros.
- Efectuar los cortes de documentación correspondientes a todos los documentos prenumerados emitidos por la entidad, que tengan efecto contable y/o presupuestario, a efecto de realizar los controles de integridad respectivos.
- Analizar las clasificaciones expuestas en los estados financieros como corrientes y no corrientes, y la adecuada exposición de las cuentas que integran cada rubro.

Procedimientos de acuerdo con el esquema de fraude

“Esquema de compras/Prueba de análisis de datos”

- Comparar las tarifas de compra de productos similares por proveedor para identificar si los productos se compraron a tasas más altas.
- Comparar las compras con los vendedores, de los pedidos para cada proveedor y los productos para identificar los patrones de preferencia de los proveedores.
- Comparar el número total de contratos por proveedor para identificar la presencia de cualquier actividad de rotación de ofertas.
- Determinar el valor promedio de los contratos ganados por vendedor para identificar si los contratos de precios altos se ganan sistemáticamente.
- Analizar si hay contribuciones caritativas y sociales significativas que están vinculadas a la adjudicación de contratos.
- Comparar los nombres de empleados, las direcciones y la información de la cuenta con la información maestra de los vendedores para identificar posibles conflictos de intereses o relaciones ocultas.

“Esquemas de ventas/Prueba de análisis de datos”

- Comparar los precios de venta y/o márgenes de productos por cliente para identificar si los productos fueron vendidos a tasas más bajas.
- Comparar los precios de venta y/o margen por empleado por cada cliente y producto, para identificar cualquier patrón de precio inusual.

- Analizar las ventas, créditos y devoluciones dañadas por vendedor e identificar los valores atípicos.
- Identificar las cuentas por cobrar pendientes y analizar la conexión de la información del cliente respectivo con empresas conocidas o listas de sanciones.

Soborno

“Pagos realizados/Prueba de análisis de datos”

- Identificar grandes reembolsos de gastos/retiros en efectivo, o aumentos de caja pequeña antes de obtener un contrato grande.
- Analizar los créditos y los productos con descuento, como el porcentaje de las ventas totales por cliente o distribuidor.
- Investigar los pagos en efectivo hechos a agentes o clientes, con énfasis en particular de los montos de pagos redondos.
- Analizar los pagos hechos a cuentas fuera del país.
- Identificar los pagos hechos a agentes que no se encuentran en las regiones de clientes/ventas.
- Analizar las descripciones de pago sin impuestos, con las palabras clave de alto riesgo como “agilizar el pago”.
- Analizar los pagos hechos por viajes excesivos, donaciones caritativas, regalos y entretenimiento.
- Analizar la tabla de cuentas para identificar las cuentas vagas o sospechosas donde se podrían cargar gastos inapropiados, como “gastos varios”, “gastos especiales”, etcétera.

“Manipulación de licitaciones/Prueba de análisis de datos”

- Revisar el número de licitaciones presentadas por contrato e investigar las ofertas únicas o excepcionalmente bajas en los contratos.
- Comprobar si hay contratos divididos con proveedores para identificar los pedidos que están por debajo de los umbrales de aprobación o de oferta.
- Verificar las licitaciones y los precios para identificar licitaciones ficticias.
- Investigar las ganancias de última oferta, las licitaciones que fueron hechas a último momento y las licitaciones presentadas después de la fecha de corte.
- Comparar el ratio del contrato adjudicado presentado por el proveedor e identificar los valores atípicos.

“Premios ilegales/Prueba de análisis de datos”

- Comparar los porcentajes de comisión por agente y/o región para identificar los valores atípicos con los porcentajes significativamente más altos.
- Identificar los contratos con pagos fijos o estructuras de comisiones inusuales en comparación con los otros contratos.
- Analizar las comisiones pagadas antes de la venta para identificar avances potencialmente inapropiados de ventas falsas.
- Identificar los pagos que son inconsistentes con los términos del contrato.
- Investigar las transacciones relacionadas con los contratos que faltan y con los contratos con vacíos o páginas perdidas.

“Extorsión económica/Prueba de análisis de datos”

- Analizar los correos electrónicos, redes sociales o fuentes en línea para identificar la propiedad o direcciones comunes.
- Analizar las actividades de fin de semana de los empleados para identificar el uso indebido de información.
- Identificar a las personas que acceden, descargan y envían la propiedad intelectual de la organización a receptores externos a la compañía.
- Identificar los contactos de correo electrónico y asociaciones fantasma.
- Analizar información de los medios sociales de comunicación para identificar la información privilegiada filtrada antes de las fechas de publicación oficial.

“Robo de dinero en efectivo/Prueba de análisis de datos”

- Conciliar dinero en efectivo con el balance en contabilidad e investigar cualquier diferencia.
- Revisar el libro mayor de caja para términos anómalos de uso de efectivo o entradas de empleados no autorizadas.
- Verificar la segregación de funciones para la contabilidad de efectivo, reconciliación bancaria y las funciones del que firma los cheques.
- Estratificar los pagos por cierta cantidad de dólares e investigar grupos, valores atípicos y cantidades de sumas redondas.
- Analizar los reembolsos de los gastos en efectivo por viajes y entretenimiento de una persona y compararlo con sus compañeros.

“Robo de efectivo antes de ser registrado/Prueba de análisis de datos”

- Revisar la secuencia de números de los libros de recibos de efectivo para asegurar que no haya números fuera de la secuencia.
- Analizar el efectivo como un porcentaje del total de los activos a lo largo del tiempo para detectar el robo de efectivo antes de ser registrado a un alto nivel.
- Inspeccionar la cuenta bancaria de un empleado con un nombre similar al nombre de la compañía.
- Inspeccionar si hay alteraciones del beneficiario del cheque o del endosante.
- Localizar el ratio de los activos a pasivos corrientes a lo largo del tiempo para identificar cualquier anomalía.
- Identificar cuentas incobrables más altas que el promedio.
- Extraer facturas con pagos parciales.
- Resumir las ventas netas de los empleados y extraer a los empleados con ventas bajas.
- Investigar las quejas de los clientes sobre los pagos que no se aplican a sus cuentas.

“Robo de efectivo/Prueba de análisis de datos”

- Comparar la lista de los recibos de efectivo enviados al cajero o al contador para enlistar los comprobantes de depósito.
- Verificar la relación entre las ventas, devoluciones y asignaciones sobre un rango relevante. (Los cambios en esta relación pueden indicar un esquema de fraude, a menos que haya otra explicación válida.)
- Revisar los registros de la compañía de la serie numérica de recibos impresos, prenumerados y verificar que estos recibos se utilicen secuencialmente (incluyendo los documentos anulados).

- Revisar la puntualidad de los depósitos de un lugar a otro a la función del tesorero.
- Comparar los ajustes del inventario con las transacciones anuladas o de reembolso resumidas por empleado.
- Preguntar si las personas que manejan el dinero en efectivo han tomado vacaciones y analizar el manejo de dinero de otro empleado durante ese tiempo.

“Esquemas de facturación/Pruebas de análisis de datos”

- Identificar las compras hechas sin la aprobación respectiva o las compras hechas de forma acelerada.
- Revisar la lista de las órdenes de compra abierta o incompleta.
- Identificar e investigar las facturas que no pasaron el proceso de tres vías (orden de compra, recibo de mercancía y la factura del proveedor) antes de que se registre el pasivo correspondiente.
- Verificar que las compras se registran en un registro de compras o en un registro de cupones antes de ser procesados mediante desembolsos en efectivo.
- Identificar las condiciones de pago en la orden de compra que no coincidan con la información del proveedor.
- Extraer proveedores con perfiles incompletos, especialmente aquéllos con números de teléfono o número de identificación fiscal perdidos o no identificados.
- Relacionar el archivo maestro del proveedor con el archivo principal del empleado en varios campos claves, tales como la dirección o el número de identificación fiscal.
- Identificar números de pedido, créditos y facturas duplicados.
- Revisar los pagos con poca o ninguna secuencia entre los números de factura.
- Identificar los desembolsos en los que la parte de aprobación de pago es la misma que la parte de aprobación de compra.

“Esquemas de nómina/Pruebas de análisis de datos”

- Enumerar a los empleados con excesivas horas de trabajo para identificar irregularidades tales como: más de 24 horas trabajadas en un solo día o significativamente más horas trabajadas que sus compañeros.
- Identificar números duplicados de depósitos, nombres de empleados, direcciones o números de teléfono.
- Identificar a las personas en la nómina sin tiempo libre para vacaciones o licencia por enfermedad.
- Identificar los cambios repentinos, significativos y análisis de patrones.
- Mapear geográficamente las direcciones de los empleados y detectar anomalías en relación con su lugar de trabajo.
- Extraer varios depósitos de nómina de la misma cuenta bancaria en un solo periodo de pago.

“Esquemas de reembolso de gastos/Pruebas de análisis de datos”

- Identificar los viajes de negocios con salidas el viernes o el sábado y los regresos el domingo o el lunes y verificar el propósito del viaje de negocio.
- Comparar la ubicación del viaje y la ubicación de los gastos.
- Aislar los montos de dólares de fuentes inesperadas (hoteles, alquiler de automóviles, etc.) e investigar por gastos fraudulentos.

- Revisar los gastos que siempre terminan en números redondos o con cantidades consistentes.
- Calcular la desviación estándar por el tipo de gasto (por ejemplo: comidas, hospedaje, alquiler de auto, etc.) e investigar cualquier cosa mayor a dos veces la desviación estándar de la media.
- Estratificar los gastos por empleado y título/puesto de trabajo para identificar los valores atípicos o inconsistentes.
- Identificar los gastos con la información requerida como fechas, horarios o propósitos de los gastos.

“Comprobar la alteración de las pruebas de análisis de datos”

- Verificar las secuencias de números de los cheques e identificar los números de cheque desaparecidos que puedan indicar un control sobre la custodia física de los cheques. (Emita los pagos de todos los cheques que faltan.)
- Comparar los cheques pagaderos a nombre de los empleados o con dinero en efectivo, fuera de los cheques normales de nómina o de gastos. (Estos desembolsos también podrían revelar conflictos de intereses, proveedores ficticios o esquemas de reembolso de gastos duplicados.)
- Analizar el registro de cheques para los números de cheques duplicados o las cantidades exactas en dólares (hasta el centavo) en la misma fecha a diferentes beneficiarios.
- Identificar los cheques sin facturas del sistema relacionado.
- Identificar las compras sin órdenes de compra y resumir por proveedor y emisor.
- Extraer los cheques manuales y resumir por beneficiario y emisor.

“Registro de desembolsos/Pruebas de análisis de datos”

- Comparar los permisos por tienda para identificar los valores atípicos.
- Resumir los reembolsos por número de tarjeta de crédito y compararlo con las compras.
- Calcular el número por parte del vendedor para identificar los valores atípicos.
- Identificar los reembolsos por montos mayores que por precio de venta.
- Identificar las transacciones con la compra y el reembolso dentro de 10 días o menos.

“Uso inadecuado de las pruebas de análisis de datos”

- Analizar las diferencias en el recuento de inventarios e identificar una mayor utilización de materiales o suministros.
- Comparar la rotación de surtido por producto y la rotación esperada e investigar la utilización mayor.
- Proporcionar el uso de los suministros o cancelaciones por mes o por departamento e identificar los valores atípicos.

“Robo de pruebas de análisis de datos”

- Comparar el conteo físico de las existencias con las cuentas de inventario computadas.
- Identificar casos de eliminación seguida de reordenamiento, lo que podría indicar la eliminación/robo de artículos utilizables.
- Resumir los artículos enviados a la basura o hechos obsoletos por el vendedor.
- Ajustar el inventario de estrategias por empleado, costos extendidos, ubicación, etcétera.
- Identificar recibos por los informes de recepción en el sistema receptor que no estén de acuerdo con los recibos por las facturas de cuentas por pagar.

- Extraer el inventario con un precio negativo o cero.
- Determinar el cambio porcentual en ventas, precio o niveles de costos por producto y proveedor.

“Pruebas analíticas de datos de ingresos ficticios”

- Comparar los descuentos o incentivos mensualmente para identificar puntas inusuales al final del cuatrimestre o del año.
- Identificar los ingresos reconocidos al cierre del periodo e invertirlos o revertirlos parcialmente.
- Analizar el margen bruto por mes e identificar cualquier valor atípico.
- Analizar las ventas hechas a clientes que tienen nombres de empresas, que suenan como clientes conocidos y que tienen campos faltantes.
- Analizar los correos electrónicos de empleados seleccionados (contabilidad o ventas) con palabras clave, relacionadas con el reconocimiento e ingresos que indiquen incentivos/presión, oportunidad y racionalización.

“Diferencias de tiempo de pruebas de análisis de datos”

- Analizar el margen bruto por mes e identificar cualquier valor atípico.
- Comparar las fechas de facturación con las fechas de envío para las grandes lagunas en el tiempo o fecha de envío anterior de la fecha de factura.
- Comparar las fechas de factura con las fechas de recepción de mercancías para detectar grandes lagunas en el tiempo o la fecha de envío antes de la fecha de factura.
- Comprobar cualquier entrada inusual de ingresos que no esté respaldada por documentos.
- Realizar un análisis de la Ley de Benford para identificar anomalías, tales como números de factura desproporcionados, que comiencen con números específicos.

“Pasivos y gastos ocultos en las pruebas de análisis de datos”

- Comparar y/o estratificar los gastos por mes y año anterior e investigar los valores atípicos.
- Analizar los gastos significativos después de las fechas de corte para identificar cualquier retraso en los registros.
- Analizar el tiempo de factura al pago e identificar facturas con tiempos inesperadamente cortos entre la factura y el pago.

“Evaluaciones de activos inapropiados/Pruebas de análisis de datos”

- Revisar las ventas de activos fijos a precios significativamente por debajo o por encima del valor depreciado.
- Identificar las ventas de activos fijos que están significativamente antes del final del ciclo de vida de la depreciación.
- Revisar el número de cancelaciones imprevistas de activos que podrían indicar una emisión sistemática en el establecimiento de depreciaciones.
- Aislar el conteo de mercancía donde los costos son mayores al precio de venta.
- Identificar el inventario sobrante u obsoleto.

2.1.3.4 Procedimientos analíticos

Los auditores forenses pueden utilizar procedimientos analíticos para obtener evidencia de auditoría, éstos consisten en el estudio y comparación de las relaciones entre la información financiera y la no financiera, esta



aplicación de los procedimientos analíticos se basa en la premisa de que, en ausencia de condiciones conocidas que indiquen lo contrario, se espera que las relaciones entre la información existan y continúen. Es decir, existe información que al ser comparada o relacionada, debería seguir un patrón esperado de comportamiento y si no lo hicieran, podría inferirse la existencia de ineficiencias, errores, fraude o actos ilegales. Los procedimientos analíticos son útiles para la identificación de:

- a) Diferencias imprevistas.
- b) Ausencia de las diferencias previstas.
- c) Errores potenciales.
- d) Fraude o actos ilegales potenciales.
- e) Otras transacciones o acontecimientos inusuales o no recurrentes.

En la siguiente tabla se presentan los procedimientos analíticos específicos, así como los procedimientos específicos que incluyen:

Ilustración 31. Clasificación de procedimientos analíticos

Procedimientos analíticos	
Generales	Específicos
1. Comparar información del periodo actual con información de periodos anteriores (Ej. Comparar presupuestos y previsiones)	• Serie de tiempo (Análisis de tendencia) • Serie de tiempo interrumpida • Comparación con presupuestos y previsiones • Prueba de razonabilidad
2. Estudiar relaciones entre información financiera y no financiera (Ej. Comparar gastos de personal comparado con cambios en el número promedio de empleados)	• Análisis de ratios • Análisis de razones financieras
3. Estudiar relaciones entre los elementos de información (Ej. Fluctuación del gasto de intereses registrado, comparado con cambios en saldos deudores)	• Análisis de relación • Análisis de regresión
4. Comparar información existente con expectativas basadas en información similar de otras unidades de la organización	• <i>Benchmarking</i>

Fuente: Elaborado por el autor.

Los procedimientos analíticos pueden realizarse usando cantidades monetarias, físicas, ratios o porcentajes; los procedimientos analíticos específicos incluyen análisis de ratios, análisis de tendencia y análisis de regresión, test de viabilidad, comparaciones periodo a periodo, comparaciones con presupuestos, previsiones e información económica externa:

- **Series de tiempo o análisis de tendencia.** Es la clasificación de valores de datos a lo largo de un periodo, permite el estudio de patrones pasados y actuales, y puede ser usada para proyectar patrones futuros; este tipo de análisis para identificar comportamiento de datos o transacciones inusuales podrían indicar un fraude.
- **Comparación con presupuestos, previsiones y otra información económica.** Consiste en comparar los datos y mediciones existentes sobre el desempeño del presupuesto y previsiones con lo presupuestado originalmente; se utiliza para evaluar el desempeño del presupuesto y el cumplimiento de las expectativas planteadas al inicio del ejercicio; así como para evaluar la eficacia de un cliente para conseguir sus objetivos, determinar si se debe investigar la existencia de un error y/o fraude.
- **Prueba de razonabilidad.** Cuando se compara un conjunto de información con otro, se espera encontrar una relación razonable entre ellos y sirve para definir si es necesario iniciar una investigación adicional por inconsistencias por encima de lo tolerable.

- **Análisis de ratios/razones.** Permite la creación de una proporción que muestra la relación entre dos tipos de unidad diferentes; se usa para comparar actividades en el tiempo, ejemplo: Número de quejas por empleado cada año o número de quejas por cada 100 empleados en cada sede; el análisis de ratios o razones permite comparar indicadores que se encuentran relacionados entre sí.
- **Análisis de razones financieras.** Una de las formas más comunes de procedimiento analítico es el análisis de razones financieras, la comparación de un elemento financiero con otro; las razones financieras se utilizan para evaluar la liquidez y rentabilidad de una organización, así como pueden ser utilizadas para identificar tendencias inusuales y, por lo tanto, la probable existencia de un fraude.

Los ratios financieros implican el uso exclusivo de los datos financieros, tanto en el numerador como en el denominador de la fracción; estos ratios son normalmente los más fáciles de calcular para las partes externas, porque la mayoría, si no es que todos los datos requeridos para realizar los cálculos, están disponibles en los estados financieros publicados de una entidad.

Los ratios mixtos implican un cálculo que incluye tanto datos financieros como no financieros; a menudo, un numerador financiero coincide con un denominador no financiero.

Los ratios y las medidas no financieras se centran exclusivamente en datos no financieros y pueden expresarse en un formato de relación tradicional o en algún otro formato, un ejemplo de esto lo incluyen las tasas promedio en las que los clientes devuelven las mercancías que han comprado y el tiempo para procesar una orden.

Como ratios mixtos, los ratios no financieros y las medidas son a menudo difíciles de calcular para las partes externas que, probablemente, no poseen los datos que se requieren, pero cuando están adecuadamente emparejados con esquemas de fraude específicos; los análisis de la proporción mixta y no financiera pueden ser armas importantes en un arsenal de detección de fraude. Uno de los principales beneficios de analizar tales relaciones es que los datos no financieros son típicamente mucho más difíciles de manejar que los datos financieros, por lo que estos índices pueden ayudar a identificar los fraudes que podrían pasar desapercibidos en el análisis de la razón financiera tradicional.

Una de las razones financieras más comunes es la liquidez, que es la habilidad económica de la organización para cumplir con sus obligaciones corrientes en su vencimiento y continuar operando a corto plazo; la liquidez ha sido vista como uno de los principales indicadores de la solidez de la organización, muchos fraudes financieros han causado una falta de liquidez y, por lo tanto, un alto en las operaciones, lo cual es el más alto riesgo del fraude.

Las siguientes razones financieras son medidas de la liquidez relativa de una organización (entre más alta la razón financiera, más alta será la liquidez) con base en los montos en el balance general:

1. La razón corriente es igual al saldo de los activos corrientes dividido entre el saldo de los pasivos corrientes.

$$\text{Razón corriente} = \frac{\text{Saldo de los activos corrientes}}{\text{Saldo de los pasivos corrientes}}$$

2. La rotación de cuentas por cobrar mide el número de veces que el saldo promedio de cuentas por cobrar se convierte en efectivo en el espacio de un año (o ciclo de estado financiero). Cuando las cuentas por cobrar no se ven reflejados en efectivo de manera esperada o continua, podría encontrarse un mal manejo del efectivo e incluso fraude en ventas o cuentas por cobrar.

$$\text{Rotación de cuentas por cobrar} = \frac{\text{Ventas a crédito netas}}{\text{Saldo promedio de cuentas por cobrar}}$$

3. La rotación de inventario mide el número de veces que el saldo promedio de inventario se convierte en efectivo en el espacio de un año (o ciclo de estado financiero). Este indicador permite identificar cambios en el inventario que son inesperados y, por lo tanto, pueden indicar en robo de inventario, fraude en ventas o en tesorería.

$$\text{Rotación de inventario} = \frac{\text{Costo de ventas}}{\text{Saldo promedio de inventario}}$$

Asimismo, otro indicador común que implica el adecuado estado de la organización o cualquiera de sus procesos o actividades es la rentabilidad, que es medida por tres porcentajes comunes basados en montos en el estado de resultados:

4. **Margen bruto de utilidad.** Es la proporción del margen bruto sobre las ventas; el asunto clave es la relación del margen bruto con el aumento o disminución de las ventas, por ejemplo, el aumento en las ventas es proporcional al aumento del margen bruto; de no ser así, pueden existir errores o fraude en el registro de ventas, ingresos o procedimientos contables.

$$\text{Margen bruto de utilidad} = \frac{\text{Margen bruto}}{\text{Ventas}}$$

5. **El margen operativo de utilidad.** Es la proporción del margen operativo sobre las ventas, algunos de los fraudes en materias primas y compras pueden identificarse mediante esta razón financiera y sus fluctuaciones inusuales comparadas con otra información.

$$\text{Margen operativo de utilidad} = \frac{\text{Margen operativo}}{\text{Ventas}}$$

6. **El margen neto de utilidad es la proporción de las utilidades netas sobre las ventas.** Este porcentaje es particularmente importante porque mide la proporción de los ingresos de la organización que puede pasar a sus dueños. Algunos fraudes sobre las utilidades, evasión fiscal u otros, pueden ser identificados por medio de esta razón:

$$\text{Margen neto de utilidad} = \frac{\text{Utilidades netas}}{\text{Ventas}}$$

Las razones financieras por sí solas revelan poco acerca de la organización o pueden darnos alguna información acerca de la existencia de un fraude; es por esto que pueden analizarse razones en conjunto o compararse entre sí, para obtener información más relevante, como son:

1. El análisis de tendencias rastrea los cambios de una razón financiera con el tiempo, por ejemplo, los últimos tres años fiscales; esto puede indicar cambios en el tiempo y determinarse las causas de las mismas.
2. El análisis de periodo a periodo compara el rendimiento para tiempos similares, por ejemplo, el tercer trimestre del año en curso y el tercer trimestre del año anterior.
3. El análisis de industria compara las razones financieras de la organización con las de sus competidores o con los promedios publicados para toda la industria. Éstos deben utilizarse con precaución, ya que diferentes empresas en la misma industria pueden tener distintas estructuras de costos.

Otros procedimientos analíticos

El análisis de regresión determina el grado de relación, si existe alguno entre dos variables, como entre ventas y costo de ventas; el grado de relación puede utilizarse como punto de referencia para probar la razonabilidad en el futuro; el análisis de varianza estudia la diferencia (favorable o no favorable) entre un monto basado en un resultado actual y el monto presupuestado correspondiente. Es un método de planificación y control que centra la atención en las causas de desviaciones significantes de las expectativas. Los anteriores tipos de análisis permiten establecer banderas rojas que junto con la mente creativa e investigadora del auditor forense permitirá prevenir y detectar el fraude.

2.1.3.5 Procedimientos para la detección de tipos específicos de fraude

Procedimientos orientados a detectar sustracción de activos

- Conciliaciones bancarias.
- Revisar partidas de cuentas vigentes en contra de cuentas antiguas.
- Efectuar arquezos de caja inesperados sin previo aviso.

- Efectuar arqueos de documentos valorados de la organización.
- Inspección física de los activos de la organización.
- Solicitar confirmaciones de terceros de las principales cuentas de balance.
- Evaluar que las compras y/o ventas relacionadas con el giro del negocio estén de acuerdo con las condiciones del mercado.
- Evaluar las utilidades de las cuentas inactivas.
- Revisar los cargos a la cuenta de resultados.
- Verificar si todas las cobranzas son depositadas íntegramente.
- Exanimación y verificación física del inventario.

Procedimientos orientados a la detección de fraude de facturación

- Folios no consecutivos.
- Cantidades repetidas en las facturas, incluso con decimales.
- Facturas en blanco o con datos a lápiz.
- Facturas con errores minúsculos o con falta de datos.
- Compra de los mismos artículos en un corto periodo.
- Facturas con RFC falso o incompleto.
- Facturas con vigencia vencida.
- Detectar facturas de venta que entran como compras valoradas exageradamente.

Procedimientos orientados a la detección de crimen de cuello blanco

- Efectuar un análisis de la situación financiera y económica de la empresa que nos permita determinar si las decisiones tomadas por la alta dirección generaron valor o, de lo contrario, lo destruyeron; la situación financiera y económica debe ser comparada tanto con los planes estratégicos de la empresa y contrarrestada con la tendencia del sector al que pertenece el negocio.
- Analizar los resultados obtenidos por cada uno de los centros de ingreso de la empresa e incidir sobre las líneas de negocios que originaron pérdidas y destruyeron el valor del negocio de la misma.
- Preparar indicadores de gestión, volumen de negocios, productividad, tipos de ingresos, gastos y determinar si están de acuerdo con el sector económico y con los planes estratégicos de la empresa.
- Solicitar las actas de la dirección y de la junta general de accionistas para determinar si todos los acuerdos de inversión y de negocio fueron debidamente ejecutados por las respectivas gerencias.
- Investigar si las gerencias constituyeron empresas *outsourcing* y si éstas prestan servicios a las mismas, con la finalidad de determinar si estos servicios están de acuerdo con las necesidades de la compañía y a precios de mercado.
- Investigar sobre los niveles patrimoniales que han obtenido los gerentes desde su permanencia en la empresa, de tal manera que se aduzcan incrementos patrimoniales no justificados.
- Revisar los legajos personales y extraer los nombres de los familiares y de las participaciones que pudieran tener en otras empresas para tomarles en cuenta cuando se revisen compras, proveedores, castigos, préstamos, descuentos otorgados, etcétera.
- Analizar la evolución de la estructura de los activos para determinar si éstos han crecido y generado valor, debiendo efectuarse desde la fecha en que se nombró al gerente general y su equipo gerencial.

- Evaluar las provisiones contables determinadas y aprobadas por la dirección.
- Analizar con detalle las razones de las cuentas de clientes que son castigadas y si éstas tienen alguna relación con las gerencias.
- Evaluar los motivos que originan que una empresa o persona tengan participaciones accionarias en otras compañías y efectuar el seguimiento de las rentabilidades obtenidas en dicha participación.
- Verificar si los gerentes tienen préstamos que han sido aprobados por la dirección.
- Verificar si se han efectuado con los recursos de la empresa, préstamos a compañías relacionadas con familiares de las gerencias.
- Verificar si los pagos efectuados por compra de inmuebles están de acuerdo con los precios del mercado.
- Verificar si existen facturaciones incluidas en los resultados y que en los próximos días son anuladas de tal manera que pretenden dar la apariencia de que las metas presupuestales están siendo cumplidas.
- Verificar si los resultados obtenidos en las ventas de activos son reconocidos en el periodo.
- Verificar si la gerencia adquiere posiciones especulativas ocultas de tipo de cambio, precios de mercado y que éste sirva de base para su registro contable.

Procedimientos orientados para la detección de fraude en la nómina

- Cotejar el número de empleados de la nómina contra la lista de personal activo.
- Cotejar el número de personal activo contra el personal inscrito en el seguro social.
- Verificar las tarjetas de reloj checador contra las horas totales pagadas.
- Verificar si el tabulador de puestos cumple con el monto pagado por nómina.
- Verificar el importe total de sueldos con el fin de cotejar si los montos pagados al seguro social son correctos.
- Verificar si las firmas de los recibos de nómina corresponden al empleado.
- Pagos injustificados por compensaciones o viáticos sin documentación comprobatoria.

2.1.3.6 Técnicas de observación

Permite obtener información para contar con una mejor comprensión de la entidad auditada, principalmente en casos en donde se da interacción con el usuario; también puede brindar ayuda en la fase de examen, para verificar la existencia de recursos físicos, resultados tangibles o falta de los mismos en programas implementados; la observación de personas requiere atención, con el fin de asegurar que las observaciones son correctas, comparables y representativas.

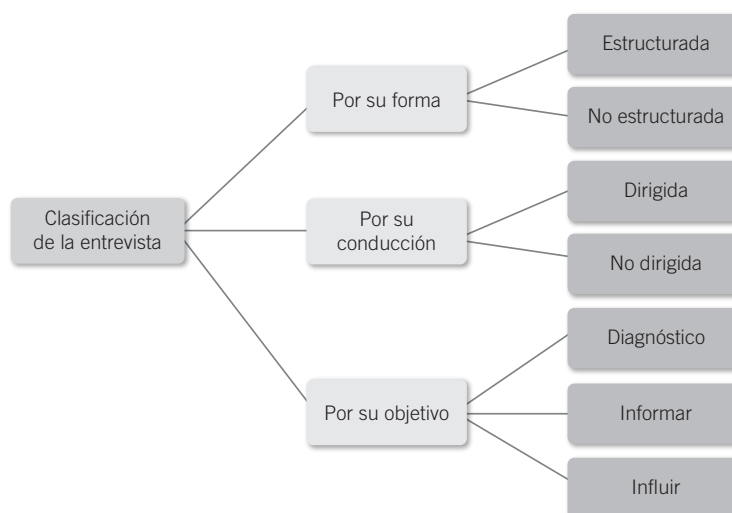
La técnica se limita por el efecto que pueda tener el acto de ser observado en el desempeño del proceso o procedimiento.

2.1.3.7 Técnica de entrevista e interrogatorio

Entrevista

Es un método para investigar aspectos de la vida del entrevistado, es un proceso de comunicación e interacción, en el cual una de las partes es un experto en un área y cuyo propósito es obtener información. La entrevista tiene como objetivo obtener información de una persona con un fin determinado, suele seguir una pauta, gira en torno a temas establecidos relevantes para los objetivos; existen dos roles definidos: el entrevistador y el entrevistado; el primero debe tener control directo, así como control de las interacciones que se establecen y hacer que ellas vayan dirigidas a obtener el objetivo propuesto. La entrevista puede clasificarse como:

Ilustración 32. Clasificación de la entrevista

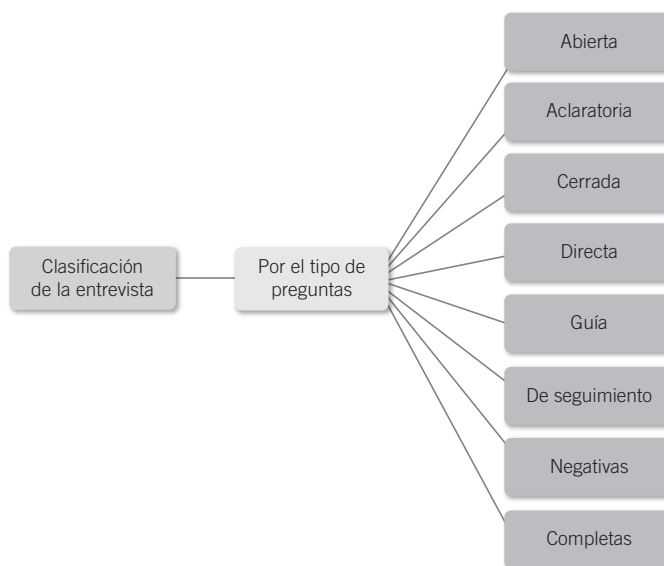


Fuente: Elaborado por el autor.

- **Estructurada.** Se planea previamente con objetivos y resultados previstos.
- **No estructurada.** Se va desarrollando conforme se presentan las circunstancias, no hay planeación.
- **Dirigida.** Se guía al entrevistado sobre tópicos específicos, sin permitir que aborde otros temas.
- **No dirigida.** Se permite al entrevistado expresarse libremente.
- **Diagnóstico.** Investigar o recoger hechos, averiguar o aclarar algo acerca del sujeto.
- **Informar.** Motivar, enseñar o demostrar algo al sujeto.
- **Influir.** Modificar el comportamiento o las actitudes o aconsejar al sujeto.

Asimismo, por el tipo de preguntas que se realizan puede clasificarse como:

Ilustración 33. Clasificación de la entrevista por tipo de preguntas



Fuente: Elaborado por el autor.

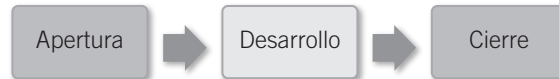
- **Abierta.** Con una amplia libertad para plantear las preguntas o para las intervenciones, el entrevistado es libre de responder lo que quiera sobre el tema.
- **Aclaratoria.** Permiten clarificar cualquier punto de la respuesta del entrevistado.
- **Cerrada.** Se plantean las preguntas de tal manera que la respuesta debe ser específica, da un mínimo de libertad y puede tener poca profundidad.
- **Directa.** Se realizan en la etapa final con el propósito de conseguir una confesión.
- **Guía.** Permiten confirmar información conocida y la veracidad de las respuestas del entrevistado.
- **De seguimiento.** Se realizan para ampliar la información obtenida.
- **Negativas.** Representan un proceso cognitivo complejo, lo que facilita al entrevistado mentir.
- **Completas.** Realizar varias preguntas al mismo tiempo o replantear una pregunta antes de obtener la respuesta.

Es necesario elaborar un plan para cumplir los objetivos propuestos, escuchando del entrevistado la información más relevante. El auditor forense se puede encontrar con tres tipos de entrevistados:

1. El neutral, quien no tiene nada que ganar o perder.
2. El cooperador, dispuesto a ser entrevistado, motivado por una variedad de razones.
3. El hostil, que dice medias verdades por temor a ser descubierto como el autor del fraude.

El entrevistador debe ser honesto e íntegro, tener la capacidad de escuchar, mantener el autocontrol, no prejuizar al entrevistado, no tratar de impresionar, controlar sus emociones, ser serio (no rígido) y paciente.

La entrevista sigue un proceso lógico que se organiza en tres etapas de manera clásica: apertura, desarrollo y cierre.



Durante la apertura se establece el encuadre, es decir, el tiempo, lugar y rol del entrevistador; se define el tipo de trabajo, estrategias a implementar, se establecen reglas y características de las sesiones y se establece la empatía entendida ésta como un interés auténtico e imparcial hacia su situación. El desarrollo consiste en realizar la investigación de la vida del entrevistado:

1. **Aclaraciones.** Define o despoja de subjetividad al entrevistado.
2. **Confrontación.** Permite relacionar contradicciones, incongruencias, etcétera.
3. **Interpretaciones.** Esclarece las resistencias y contenidos inconscientes.

Se debe considerar si se han cumplido los objetivos de la sesión de la entrevista, se puede propiciar un análisis con el entrevistado para evaluar los logros, el cierre se realiza de:

- a) Cada encuentro.
- b) Final del proceso.

Interrogatorio

Existen diferencias significativas entre la entrevista y el interrogatorio, mismas que son importantes de aclarar para efectos de su uso en la auditoría forense; el objetivo del interrogatorio es obtener información acerca de un hecho, mientras que en la entrevista se busca conocer a la persona del entrevistado. Por las características del interrogatorio es importante considerar:

- El ambiente donde se va a desarrollar el interrogatorio.
- Los interrogadores.

- Tipo y redacción de las preguntas y su secuencia lógica.
- Preguntas para validar las respuestas del interrogado.

El éxito en el logro de los objetivos planificados en un interrogatorio reside en el cuidado que deben poner sus ejecutores en la programación; el interrogador debe hacer una examinación previa de todas las personas que tienen conocimiento al respecto y tomar declaraciones de testigos e informantes.

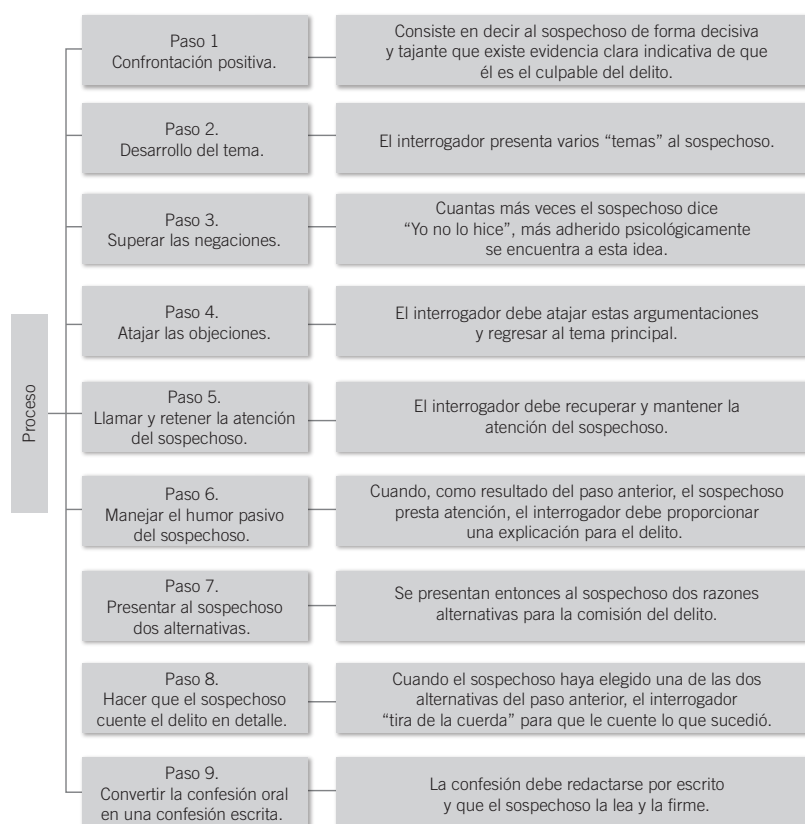
La llamada técnica Reid de interrogatorio parte de la base de que el sujeto es sometido a interrogatorio y está mintiendo al negar su implicación en el delito.

El sospechoso miente, porque decir la verdad tendría consecuencias negativas para él, y no cederá hasta que las consecuencias de una confesión sean mejores a las derivadas de mantener su engaño; el interrogador cuenta con un aliado: la socialización de que mentir es moralmente incorrecto, hace que el mentiroso experimente un conflicto interno que se traduce en ansiedad y el sospechoso siente la necesidad de liberar dicha ansiedad.

La meta del interrogador consiste en incrementar dicha ansiedad y reducir al mismo tiempo las consecuencias negativas percibidas de la confesión; esto lo hace mediante un interrogatorio en nueve pasos, destinado a lograr que el sospechoso confiese.

El interrogatorio debe llevarse a cabo en una pequeña habitación aislada a prueba de ruidos, sin mobiliario ni ornamentación alguna y sin distracciones; asimismo, debe contener sólo dos o tres sillas poco confortables, sin brazos y con el respaldo a 90° del asiento y una mesa, es preferible que la habitación tenga un espejo unidireccional para que otros policías puedan observar, desde otra habitación, signos de fatiga, nerviosismo, desazón, etcétera. En este contexto, los interrogadores someten al interrogado al siguiente proceso:

Ilustración 34. Proceso de interrogatorio



Fuente: Garrido, 2006.

En la ilustración 34 se clasifican los nueve pasos dentro de dos categorías fundamentales: maximización y minimización; la primera consiste en emplear técnicas que intimiden al sospechoso y la minimización consiste en “embaucar” al sospechoso, ofreciéndole una falsa seguridad.

Se reestructuran las estrategias bajo la forma de tres procesos generales: aislamiento, enfrentamiento y minimización; con respecto al aislamiento, se retiene al sospechoso contra su voluntad y se le introduce en una habitación especial para interrogarlo; una vez que el sospechoso está aislado empieza el enfrentamiento. Es acusado de haber cometido un delito, sus negaciones son interrumpidas, sus explicaciones no son escuchadas y es bombardeado con pruebas que le incriminan; finalmente, cuando el sospechoso se encuentra en un estado de desesperanza, se entra en la minimización: se le plantea la confesión como un medio de escapar de la situación.

Riesgos de las técnicas de interrogatorio

Las tácticas de interrogatorio recomendadas están basadas en la experiencia de los autores, en la investigación científica y, por lo tanto, no están exentas de riesgos, entre las que se encuentran generar admisiones y confesiones falsas.

Hay una serie de características individuales que puede poner a determinadas personas en una situación de mayor vulnerabilidad a la presión ejercida durante los interrogatorios, incrementando la posibilidad de que hagan confesiones falsas. Estas características son la corta edad, la escasa inteligencia y el retraso mental, las enfermedades mentales, la sugestionabilidad y la sumisión.

- **Edad.** En los últimos años se han hecho estudios para determinar en qué edad las personas tienden a realizar confesiones falsas, se detectó que las confesiones falsas que se produjeron fueron de personas jóvenes y adolescentes. Entre las razones más frecuentes que los adolescentes citaron para haber hecho una confesión falsa estaba “la creencia de que, tras confesar, podrían irse a casa”.
- **Inteligencia, retraso mental y enfermedades psiquiátricas.** Las personas con escasa inteligencia, retraso mental y enfermedades psiquiátricas, son más susceptibles a preguntas sesgadas, confabulan más y muestran alta necesidad de aprobación con el interrogador.
- **Sugestionabilidad.** Es la variable que más se ha estudiado. Las puntuaciones en sugestionabilidad se correlacionan con la inteligencia, ansiedad, memoria, falta de asertividad, entre otras.
- **Sumisión.** Es el deseo de agradar y de proteger su autoestima, en presencia de otras personas, así como el deseo de evitar la confrontación y el conflicto con los demás, especialmente de aquellos que son autoridad.

Consecuencia de declaraciones falsas

El peligro de obtener falsas confesiones durante los interrogatorios, así como los indudables perjuicios que éstas acarrearán al sospechoso, obligan a tomar medidas de prevención; tales medidas deben ser de tipo legal; asimismo, hay otras medidas que se pueden añadir a las existentes. Se señalan a continuación algunas medidas que la legislación española ha tomado en cuenta para la problemática de las confesiones falsas:

- **Instruir a la policía en lo concerniente a las confesiones falsas.** Muchas de tales confesiones son obtenidas por policías bien intencionados que ignoran los peligros que conllevan ciertas técnicas de interrogatorio. Se señalan cuatro ámbitos en que la policía debería de recibir información:
 - La pobre relación entre el comportamiento corporal y la culpabilidad o inocencia del sospechoso.
 - La existencia, diversidad y causa de las confesiones falsas y cómo funcionan las tácticas coercitivas y el interrogatorio que a veces se emplean.
 - Cómo diferenciar entre confesiones falsas y verdaderas.
 - Cómo interrogar a personas pertenecientes a grupos vulnerables.
- **Limitar por ley el tiempo de custodia del sospechoso.** La detención preventiva debe prolongarse sólo durante el tiempo necesario para el esclarecimiento de los hechos y, en ningún caso durante

más de 72 horas; pasado este tiempo, el detenido debe ser puesto en libertad o pasar a disposición judicial.

- **Limitar por ley la duración del interrogatorio y el horario en que éste se realice.** Cuando el examen del imputado se prolongue durante mucho tiempo o cuando se le hayan hecho tantas preguntas que haya perdido la serenidad de juicio para seguir contestando, se le dará un tiempo para descansar y recuperar la calma.
- **Evitar el empleo de tácticas coercitivas de interrogatorio.** Todo detenido debe ser informado de sus derechos, como son: guardar silencio, no declarar contra sí mismo y no confesarse culpable.
- **Evitar proporcionar al sospechoso información sobre el delito durante el interrogatorio.** El detenido debe ser informado desde un primer momento de los hechos que se le imputan, no conviene darle toda la información sobre el delito hasta haber obtenido de él toda la información fiable que pueda proporcionar.
- **Exigir legalmente la presencia de un abogado durante el interrogatorio.** Asistencia de un abogado.
- **Filmar en video el interrogatorio.** Grabación audiovisual del interrogatorio y recogiendo el interrogatorio completo. Las ventajas de esto son:
 - Guardar un registro literal y exacto de la declaración del imputado y las circunstancias en que ésta se produjo.
 - Garantizar el cumplimiento de la normativa concerniente al modo en que deben hacerse los interrogatorios.
 - Atajar las quejas o demandas del imputado o la defensa, argumentando presión o malos tratos durante el interrogatorio.
- **Comparar la información proporcionada por el interrogatorio con los hechos objetivos del delito.** No solamente es necesario que se comenten las afirmaciones del interrogatorio, al igual es necesario:
 - Comparar la información proporcionada en la confesión con los hechos objetivos del caso que sólo el culpable y la policía deberían conocer.
 - Examinar si la confesión describe con exactitud elementos poco comunes del delito.
 - Comprobar si la confesión conduce a nuevos hallazgos.
 - Examinar si la confesión explica anomalías o ciertos aspectos del delito.
 - Examinar si las pruebas físicas o médicas confirman la confesión.
- **Desconfiar de expresiones en la confesión del interrogado.** Pueden reflejar que el imputado no está seguro de ser realmente el autor de los hechos y que confiesa bajo presión o en un estado de confusión.
- **Establecer legalmente que nadie puede ser condenado sólo sobre la base de su confesión.** Necesita haber evidencia incontrovertible de su culpabilidad.

2.1.3.8 Técnicas de análisis asistidas por computadora

Las Técnicas de Auditoría Asistidas por Computador (TAAC's) son un conjunto de técnicas y herramientas utilizadas en el desarrollo de las auditorías informáticas, con el fin de mejorar la eficiencia, alcance y confiabilidad de los análisis efectuados por el auditor.

Las TAAC's pueden posibilitar pruebas más extensas de las transacciones electrónicas y archivos de cuentas confiables para que el auditor sustente sus observaciones y recomendaciones. Las TAAC's pueden ser usadas en:

- Selección de muestra de archivos electrónicos clave.
- Elección de transacciones con característica específicas.
- Análisis de información.
- Procedimientos analíticos.

A continuación se describen algunas de las técnicas de análisis de datos asistidas por computadora más utilizadas en la auditoría forense.

Minería de datos

Es el descubrimiento de patrones, relaciones y tendencias mediante análisis de gran cantidad de datos; el proceso de descubrir conocimiento interesante de grandes cantidades de datos almacenadas en bases de datos u otro repositorio de información. La minería de datos puede definirse como una extracción de información desconocida no trivial y potencialmente útil de una gran cantidad de información.

Los objetivos de la minería de datos son procesar automáticamente grandes cantidades de datos crudos, identificar los patrones más significativos y relevantes y presentar los patrones como conocimiento apropiado para satisfacer las metas del usuario. La minería de datos es útil principalmente para predecir, por medio de algunas variables o campos de la base de datos, valores desconocidos o futuros y para encontrar patrones que describan la información.

Análisis de texto

Es el proceso utilizado para coleccionar datos para explicar, entender, o interpretar una situación o acciones o pensamientos de una persona; esto implica la extracción de información de datos de texto estructurados que pueden ser utilizados para revelar patrones, sentimientos y relaciones sentimentales que pueden ser indicativos de fraude. El análisis de texto involucra en la examinación lo siguiente:

- Palabras clave.
- Comunicación por correo electrónico.
- Mensajes de texto.
- Contenido de los medios o redes sociales.

Por ejemplo, un análisis de comunicaciones por correo electrónico puede ayudar al examinador de fraude a medir la presión/incentivos, oportunidades y racionalización para cometer un fraude en la organización. Este tipo de herramienta puede analizar datos cuantitativos y cualitativos:

- **Datos cuantitativos.** Son aquellos que pueden ser expresados cuantitativamente y fácilmente medibles. (Ej. Cantidades exactas, mediciones, temperatura, costos, porcentajes, etcétera.)
- **Datos cualitativos.** Datos compuestos por palabras, observaciones y descripciones más que de números. Proporcionan contexto o perspectiva de un hecho potencial. (Colores, sentimientos, texturas, rasgos físicos y descripciones.)

Asimismo, los datos se clasifican en datos estructurados, no estructurados y semiestructurados, esto con el fin de identificar la manera más adecuada para su análisis.

- **Datos estructurados.** Consiste en datos de reconocible y predecible estructura, reside en un campo fijo, un registro o un archivo, son predefinidos, legibles por una máquina y localizables. (Ej. Sistemas de empresa, números de seguridad social, números telefónicos y datos económicos.)
- **Datos no estructurados.** Datos que se encuentran en la naturaleza y no han sido procesados dentro de un formato estructurado. (Ej. Correos electrónicos, mensajes instantáneos, videos, aplicaciones de teléfonos inteligentes o tabletas, textos, documentos, imágenes, páginas web, etcétera.)

- **Datos semiestructurados.** Son una combinación de los antes mencionados, estructurados y no estructurados, contienen datos que son estructurados pero incrustados dentro de datos no estructurados.

Algunas organizaciones están aplicando tecnología al texto o “extracción de texto” para conseguir el mayor valor de ambos datos, estructurados y no estructurados; la extracción de texto es una forma de análisis de texto que utiliza tecnología y software para analizar textos; éste involucra el tratamiento de textos no estructurados en un formato que puede ser analizado por sistemas computacionales. El análisis de texto abarca distintos enfoques; éstos incluyen técnicas que eligen palabras o frases, etiquetan y categorizan documentos y extraen palabras o frases significativas, mediante la revisión de correos electrónicos, se puede ganar suficiente entendimiento del contexto detrás de la motivación para la escena de fraude, incluyendo las acciones tomadas, la razón fundamental o intento por tomar ciertas decisiones.

Ya enviado, formal o informalmente, un correo provee de una visión en cuanto a la escena del fraude; ayuda a responder el quién, qué y cuándo de un fraude. Existen técnicas que se utilizan en el análisis de texto de correos electrónicos:

- **Análisis de lagunas.** Se aplica al identificar correos eliminados en alguna fecha específica. Eliminar correo indica que se quiere ocultar algo.
- **Actividades en tendencia.** La temporada cuando los estados financieros son reportados podría ser una manera de detectar una escena de fraude, observar los correos, las tendencias de actividades antes de que los libros contables sean cerrados y después de finalizar el periodo contable.
- **Si los estados financieros están manipulados.** Éste es el momento en que ocurre el fraude y se puede detectar en correos con tendencias sospechosas de fraude entre distinta persona.
- **Búsqueda por palabras clave.** Los examinadores de fraude podrían utilizar una lista de palabras relacionadas específicamente con el fraude de estados financieros, esta lista llevada al análisis de correos electrónicos podría arrojar indicios de fraude.

Ley de Benford

La Ley de Benford es una herramienta que apareció como una solución en la búsqueda de fraude, esta teoría fue descubierta en 1881 por el señor Simón Newcomb, quien observó que en una tabla de logaritmos, las hojas que más utilizaba la gente eran las que empezaban por 1, 2 y 3; esto lo llevó a investigar sobre el tema y descubrió que los números responden a una ley natural en la que los que empiezan por 1 tienen una frecuencia mayor que los que empiezan por 2 y éstos, a su vez, una frecuencia mayor a los que empiezan por 3 y así sucesivamente hasta el 9. Posteriormente, en 1938 Frank Benford realizó una comprobación empírica de la ley con un total de 20,229 números agrupados en 20 muestras de gran diversidad y, a partir de sus resultados empíricos, postuló la “Ley de Benford”.

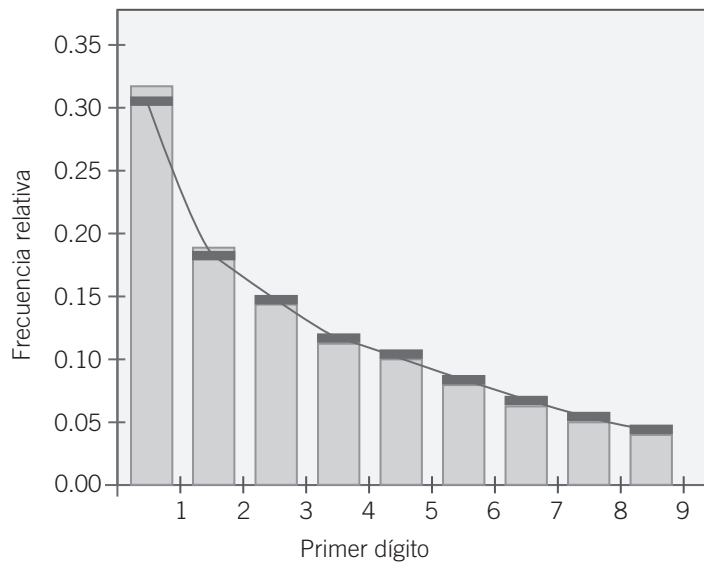
Resultado:

	Estado	Municipio	Valor	Dígito
1	A	1	2,048	2
2	A	2	9,592	9
3	A	3	185	1
4	A	4	1,503	1
5	A	5	175	1
6	A	6	734	7
7	A	7	807	8

Posteriormente se realiza el análisis de la Ley de Benford por municipio:

Dígito	Frecuencia absoluta	Frecuencia relativa	Porcentaje	Benford	Diferencia
1	2,559	0.32	31.56%	30.10%	1.46%
2	1,503	0.19	18.53%	17.61%	0.92%
3	992	0.12	12.23%	12.46%	-0.23%
4	731	0.09	9.01%	9.69%	-0.68%
5	635	0.08	7.83%	7.92%	-0.09%
6	540	0.07	6.66%	6.69%	-0.03%
7	456	0.06	5.62%	5.80%	-0.18%
8	358	0.04	4.41%	5.12%	-0.71%
9	335	0.04	4.13%	4.58%	-0.45%
Total	8,109	1			

Mediante la siguiente gráfica, se puede notar que no se encuentran diferencias significativas entre la distribución de la población y la Ley de Benford.

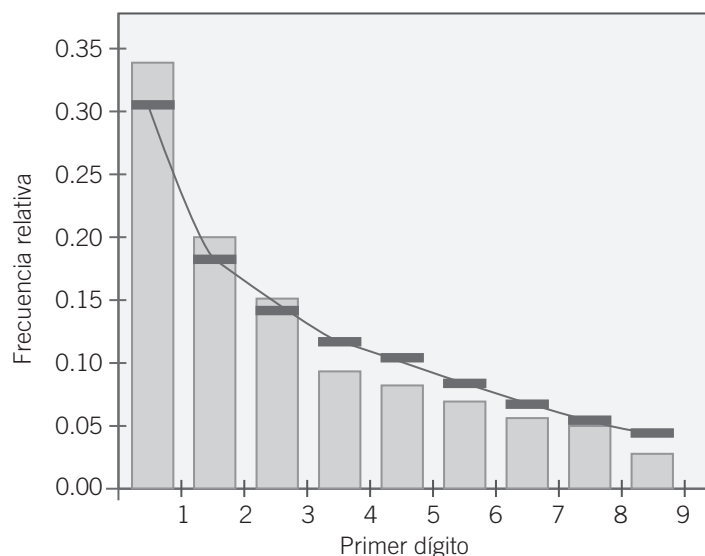


No obstante, si se toma en consideración únicamente los municipios de un estado, podremos ver mayores inconsistencias como se muestra a continuación:

Estado X

Dígito	Frecuencia absoluta	Frecuencia relativa	Porcentaje	Benford	Diferencia
1	91	0.33	33.33%	30.10%	3.23%
2	54	0.20	19.78%	17.61%	2.17%
3	37	0.14	13.55%	12.46%	1.09%
4	21	0.08	7.69%	9.69%	-2.00%
5	18	0.07	6.59%	7.92%	-1.33%
6	16	0.06	5.86%	6.69%	-0.83%

Dígito	Frecuencia absoluta	Frecuencia relativa	Porcentaje	Benford	Diferencia
7	13	0.05	4.76%	5.80%	-1.04%
8	15	0.05	5.49%	5.12%	0.37%
9	8	0.03	2.93%	4.58%	-1.65%
Total	273	1			



Como se observa, son más notorias las diferencias en los datos poblacionales respecto a la expectativa estadística que propone la Ley de Benford, dado que los datos de un solo estado se sesgan menos que al realizar el análisis con el total de la población.

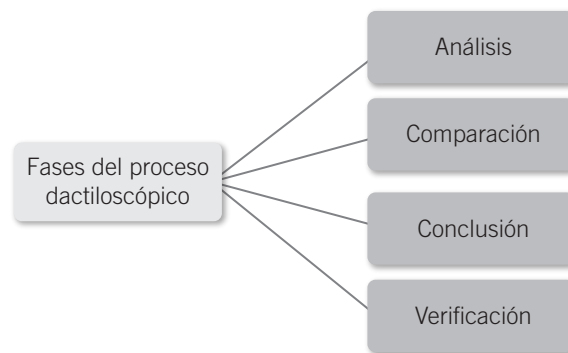
2.1.3.9 Disciplinas de apoyo

Dactiloscopia

Método de identificación basado en el estudio y clasificación de las huellas digitales presentes en los dedos de las manos; es uno de los métodos más confiables dentro del proceso de identificación, debido a las características que tienen las huellas dactilares, siendo éstas:

- Inmutabilidad (perennes, no cambian) de los dibujos dactilares desde que aparecen en la vida intrauterina.
- Inalterabilidad a lo largo de la vida.
- Variabilidad, característica de la naturaleza humana, pues no existen dos sujetos con la misma huella dactilar.
- Posibilidad de clasificación, debido a que se facilita su archivo y ordenación, de forma que pueden ser localizados de manera sencilla.

Ilustración 35. Fases del proceso dactiloscópico



Fuente: Elaborado por el autor.

- **Análisis.** Estudio de huellas dubitadas.
- **Comparación.** Confrontación de las huellas dubitadas e indubitadas.
- **Conclusión.** Análisis del proceso comparativo, en donde se llega a un resultado.
- **Verificación.** Como parte del proceso investigativo, se deben realizar repeticiones.

Grafoscopía

Las funciones del perito en grafoscopía son las siguientes:

- Obtener pruebas de escritura de las personas cuya firma o manuscrición se atribuye.
- Obtener de ser posible, documentos con contenido contemporáneo al impugnado.
- Examinar la temporalidad de los documentos.
- Verificar que se trate de documentos originales, dictaminar sobre la autenticidad o falsificación de las firmas o manuscritos sometidos a peritación.
- Determinar el origen gráfico tras un análisis minucioso y técnico, no siempre la mano que trazó se utiliza como medio de expresión gráfica, puede ser cualquier parte del cuerpo.

Documentoscopía

Estudio integral de un documento, desde el punto de vista de su autenticidad o alteración; analiza e investiga, mediante metodología e instrumental adecuado, todo tipo de documentos con el fin de determinar su autenticidad o falsedad, en cuyo caso averigua en qué consiste ésta, así como las alteraciones y manipulaciones sufridas. En un documento se consideran para su estudio:

- La tinta, en sus diversas clases.
- El tiempo como elemento subjetivo e intangible, muy difícil de valorar, es también el menos conocido porque no es visible y deja muy pocas trazas sobre el documento.
- En general el texto, firma, tinta y receptor tienen que estar relacionados con la fecha de producción del documento.
- Los mecanismos de alteración de documentos: borradura, raspadura, lavado, adición y falsificación.

2.1.4 Informe

Los dictámenes de los auditores forenses se deben basar exclusivamente en las pruebas que obtuvieron durante el trabajo de campo, cumpliendo con las normas internacionales de auditoría para su presentación y exposición. Los informes deben contener los antecedentes del caso en cuestión, descripción de los procedimientos llevados

a cabo y del alcance del trabajo, así como de las limitaciones que se hayan presentado, análisis y explicación de las pruebas obtenidas y, conjuntamente con su opinión, el auditor forense debe detallar las recomendaciones.

El dictamen debe ser claro, preciso y detallado; en él se explicarán los exámenes, experimentos e investigaciones; el dictamen emitido por el auditor debe contar con elementos básicos para su presentación con el propósito de garantizar cumplimiento normativo y calidad de la información puesta a consideración; por lo tanto, debe contener:



2.1.5 Monitoreo

Esta última fase tiene por finalidad asegurar que los resultados de la investigación forense sean considerados según sea pertinente y evitar que queden en el olvido, otorgando a los perpetradores del fraude la impunidad. El monitoreo puede consistir en el seguimiento al proceso legal de posibles fraudes comprobados por medio de la auditoría o monitoreo de la implementación de nuevos controles antifraude, también se relaciona con el seguimiento a las acciones recomendadas a la gerencia para la prevención de futuros actos fraudulentos.

2.1.6 Proceso legal

Debido a que el auditor forense podría participar en diversos procedimientos legales en los que será de gran relevancia la adecuada cadena de custodia y calidad de las evidencias presentadas, en el siguiente apartado se mencionan algunos procedimientos posteriores a la auditoría que, al recopilar la evidencia, el auditor deberá considerar.

Juicios y audiencias

Ya sea para la acusación o defensa en una causa penal o el demandante o demandado en un caso civil; la complejidad de cualquier caso dependerá de las cuestiones planteadas. Algunos casos sólo requerirán una pequeña cantidad de tiempo para estudiar y testificar, mientras que en otros casos se necesitarán muchas horas de estudio y de testificar. En cualquier caso, el testimonio de los contadores forenses proporcionará la base para las decisiones de los jueces. El auditor forense será llamado a declarar en los siguientes tipos de procedimientos legales.

Juicios penales

En los juicios penales, el auditor forense testificará sobre el patrimonio neto y los gastos del acusado, ya sea para la acusación o la defensa; esto abarcará mucho tiempo para estudiar y testificar en corte. Existen otros casos que implican el rastreo de fondos y activos.

Juicios civiles

En los juicios civiles, normalmente el auditor forense testificará sobre las estadísticas financieras del demandante o del demandado. La mayoría de los casos suelen involucrar litigios sobre el impuesto sobre la renta o la división de activos de divorcio y/o la capacidad de hacer pensión alimenticia o manutención de los niños. El tiempo requerido va a depender de la complejidad del caso.



Audiencias

El auditor forense testificará ante un juez, no estará el jurado presente; en los casos penales, el testimonio estará dirigido a la situación financiera del demandado o a sus asuntos financieros; en los casos civiles, el auditor forense testificará sobre la condición financiera del demandante o del demandado o la capacidad de pagar una demanda.

Declaración

El auditor forense dará testimonio sobre algún tema que involucre la litigación entre dos partes.

Declaración jurada

En el caso de una declaración, el auditor forense dará una declaración jurada sobre una cuestión particular; no hay juez o jurado presente, ésta es una situación unilateral, la declaración jurada se da en respuesta a preguntas y respuestas que un abogado le pide a su cliente o al gobierno.

Preparación para testificar

Al prepararse para testificar se pueden seguir los siguientes pasos:

1. Discutir con el abogado lo que se espera, cómo se va a usar su testimonio y cuándo se espera que testifique.
2. Revisar todos los documentos disponibles relacionados con la cuestión que se litiga.
3. Discutir su testimonio con el abogado, preguntar qué línea de preguntas se usará para desarrollar el caso y obtener una idea general de cómo responderá a esas preguntas.
4. Considere cuál será el enfoque del abogado opositor y las áreas que probablemente probarán durante los exámenes cruzados.

Testigo experto

Un testigo experto es una persona con amplia experiencia en algún arte, ciencia, profesión o negocio, o que tiene conocimientos en relación con asuntos que no son comúnmente conocidos por una persona común. El testigo experto expresa una opinión o responde a preguntas hipotéticas basadas en hechos que están en el expediente. El testimonio de los expertos está completamente dentro de la competencia del jurado para determinar el peso dado a tales opiniones. Los jurados no están obligados por la opinión de los expertos.

Deberes y responsabilidades

El auditor forense tiene diversas responsabilidades y deberes que debe realizar durante un procedimiento judicial. Son los siguientes:

1. En casos penales, revisar el memorando de la fiscalía.
2. En casos penales, revisar la acusación o la información que establece las acusaciones específicas del acto criminal.
3. Revisar la evidencia anticipada disponible para probar o refutar la acusación o información en casos criminales o apoyar o negar la posición del demandante o del demandado en un caso civil.
4. Comprobar la exactitud matemática de la contabilidad que se han de presentar ante el tribunal, sea penal o civil.
5. Asesorar al abogado sobre los posibles problemas contables o técnicos.
6. Determinar la manera más clara de presentar su testimonio en términos que el jurado entienda.
7. Preparar cálculos provisionales basados en la evidencia que se espera sea admitida.
8. Suministrar al abogado que está asistiendo, una declaración escrita de sus calificaciones como auditor forense y/o currículum actual.
9. Testificar sólo aquellos asuntos que son admitidos por el tribunal como evidencia, ya sea como testimonio, documentos o por estipulación.

10. Tomar notas sobre la evidencia que es admitida y preparar una lista de exhibiciones documentales de ambas partes, sea criminal o civil.
11. Alertar al abogado sobre cualquier evidencia que se pasó por alto.
12. Permitir suficiente tiempo para revisar los cálculos y revisar el testimonio de los testigos. Se deben hacer copias de esos cálculos para el jurado, corte y consejo.

Para ser un buen testigo, hay cosas que se deben hacer como son:

- Hable fuerte para que el jurado, el juez, el taquígrafo, el abogado oponente y todas las demás partes en este caso puedan oírle.
- Definir los términos técnicos y el término en un lenguaje sencillo para que el jurado, el juez y el abogado puedan entenderlos.
- Al testificar, refiérase al número de exhibición o alguna otra identificación.
- Tome el tiempo suficiente en responder las preguntas para dar una respuesta precisa y breve.
- Tenga notas adecuadas disponibles para que usted pueda testificar sobre todos los detalles.
- Caminar hasta el puesto de testigo con pasos parciales.
- Al tomar el juramento, mantenga su mano derecha alta con los dedos derechos y mire al oficial que administra el juramento. Cuando el oficial termine el juramento, usted debe contestar “acepto”.
- Piense antes de hablar.
- Cuando uno de los abogados dice “objeción” o la corte interrumpe, detenga su respuesta inmediatamente y espere hasta que el tribunal dicte su fallo.
- Sea justo y franco.
- Si usted cometió un error, admítalo y corríjalo.
- Mantenga el temperamento. Sea firme, pero flexible.
- Si no puede responder sí o no, dígalos.
- Si no sabe o no puede recordar, dígalos.
- Escuche atentamente cuando el abogado le pregunte, “¿quiere que este jurado entienda?”.
- Nunca trate de ser un testigo inteligente.
- Exprésese bien.
- Sea breve.
- Durante el receso, manténgase alejado de todo el mundo, excepto del abogado que le retuvo para testificar.
- Espere hasta que la pregunta termine para que pueda contestar.
- En el interrogatorio, no mire a su abogado.
- Mantenga sus manos lejos de su boca o cara.
- Sea serio durante los recesos y en el estrado de testigos.
- Mantenerse alejado de los abogados adversos, acusados o demandantes y sus testigos.
- Estar disponible y responder rápidamente cuando sea llamado a testificar.



Los siguientes elementos son las cosas que no debe hacer:

- No discuta el caso en los corredores.
- No memorice nada de su testimonio.
- No asiente ni sacuda la cabeza para indicar sí o no.
- No haga público ningún reparo de alegría o decepción por el resultado del caso, después de que el veredicto haya sido dictado.
- No ofrezca ninguna información.
- No muestre ninguna emoción acerca de los procedimientos como la incredulidad o el asombro.
- No se deje atrapar en la trampa de un abogado de la defensa que le pide que responda a una pregunta por ambas, “sí” o “no”. Hay preguntas que no pueden ser respondidas de esta manera, así que se debe de esperar a que el juez le dé permiso de explicar su repuesta.
- No se deje atrapar por lazos como “¿Alguna vez discutieron esto con alguien?”. Si se le pide, nombre a la gente, los abogados y las partes de la demanda.

Presentación del juicio

En la presentación de la información financiera en un juicio, ya sea civil o penal, los siguientes pasos deben seguirse para obtener el máximo efecto:

- Antes del juicio, establezca el valor de todos los artículos esperados para ir al ensayo.
- Como testigo sumario, antes de ir al estrado, tomar un receso de cuatro horas, más o menos, para repasar todos los artículos que se presentarán.
- En el juicio, tratar de conseguir el abogado para presentar su testigo en el siguiente orden:
 - Custodio de registros.
 - Investigadores de casos.
 - Probable fuente de ingresos testigos.

Esto sirve para ayudar al testigo de varias maneras:

- Primero, obtenga toda la evidencia documental por medio de la cual el testigo pueda tener tiempo para revisar los cálculos y sus pruebas.
- En segundo lugar, impresione al jurado del demandado que ha estado implicado en actividades ilegales y el efecto financiero de estas actividades.

2.2 Casos prácticos

2.2.1 Caso Supermercado Transnacional

Tipo de fraude: corrupción y sobornos

Involucrados:

Función
Denunciante
Abogada de Supermercado Transnacional (Corporativo en USA)
Principal Inculpado (Supermercado Transnacional en México)
Director Ejecutivo del Corporativo de la Transnacional
Equipo de investigación forense
Abogado contratado para realizar investigación
Vicepresidente del corporativo de la Transnacional
Auditor despedido
Director ejecutivo de transnacional en América Latina

Resumen del caso:

“Supermercado Transnacional” es una empresa multinacional de tiendas de origen estadounidense que opera cadenas de grandes almacenes de descuento y clubes de almacenes; asimismo, es la tercera mayor empresa pública del mundo. Es el principal empleador a nivel internacional, cuenta con más de dos millones de empleados, 11,000 tiendas bajo 65 marcas en 28 países y con sitios web de comercio electrónico en 11 países.

En septiembre de 2005, la abogada del corporativo con sede en Estados Unidos de América (que para efectos prácticos nombraremos “SM”) recibió un correo de denuncia por parte de un ejecutivo que se desempeñaba como abogado para la obtención de permisos de construcción que trabajaba en la filial de la compañía en México, la subsidiaria más grande de América Latina, en donde el ejecutivo denuncia esta filial de llevar a cabo una serie de sobornos para dominar el mercado, proporcionando datos, fechas y montos de los sobornos.

SM ordenó una investigación a la filial en México y envió a un equipo de investigadores, quienes encontraron evidencias de estos sobornos en papel sobre pagos sospechosos por más de 24 millones de dólares. Hallaron pruebas documentales que mostraban que altos ejecutivos de SM México no sólo sabían de los sobornos, sino que habían ocultado esta información al corporativo. El reporte arrojó que existía una presunta violación de las leyes de México y Estados Unidos de América; sin embargo, SM cerró el caso y no dio aviso a las autoridades de ambos países, incluso nombró vicepresidente de SM al ejecutivo, presunto responsable del fraude.

Desde esta fecha (2005) hasta abril de 2012, cuando un reconocido periódico de Estados Unidos de América publica un artículo en el que se muestra el caso, SM no había dado a conocer la información acerca de la investigación realizada. La publicación provocó una crisis legal, reputacional y de acciones de dicha compañía, ya que una de cada cinco de sus tiendas se encuentran en México, en donde el periódico revisó miles de documentos gubernamentales con solicitudes de permisos para apertura de tiendas en México, mismos que fueron otorgados pocos días después de pagos realizados a dos abogados.

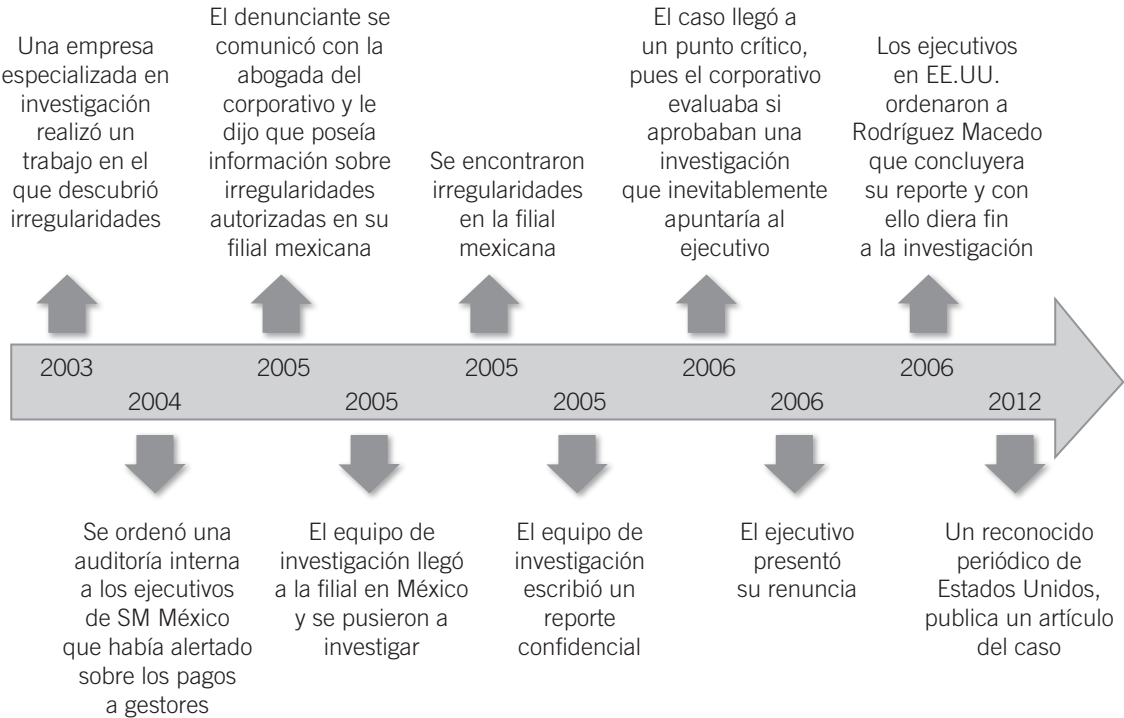
La investigación del periódico encontró evidencias creíbles de que los sobornos desempeñaban un papel significativo en la expansión de SM México y presentó los resultados de su investigación a la empresa y ésta la circuló entre sus ejecutivos, incluyendo al actual director general y su antecesor, quien se retiraría en junio de 2012. Ambos hombres se rehusaron a comentar sobre el artículo que publicó el diario.

Con el objeto de rastrear el desarrollo de la investigación desde 2005, el periódico consiguió cientos de documentos internos de la empresa, algunos de los cuales demuestran que un número importante de sus altos ejecutivos reconocían la seriedad de la denuncia. La investigación realizada por el periódico mostró más de 15 horas de

entrevistas realizadas al denunciante que laboró en SM México en 2004 después de haberse desempeñado por diez años como abogado encargado del departamento de bienes raíces de la compañía. Al ser entrevistado, declaró que durante años había ayudado a organizar los pagos; informó que enviaba a dos abogados externos a entregar sobres con dinero en efectivo, a representantes de gobierno-alcaldes y consejeros ciudadanos, planificadores urbanos, burócratas de bajo nivel, que autorizaban permisos. Cualquiera que tuviera poder para frustrar el crecimiento de SM México. Los sobornos compraron permisos de zonificación, reducciones en las cuotas de impacto ambiental y la lealtad de líderes vecinales.

El diario reseñó miles de documentos gubernamentales relacionados con solicitudes para obtener permisos de construcción de tiendas en todo México. Realizó entrevistas en profundidad a los encargados de la investigación sobre SM, quienes hablaron con la condición de no ser identificados como informantes sobre asuntos confidenciales de la empresa. Después de entregar el reporte de su investigación, estaban convencidos que lo dicho por el denunciante resultaba persuasivo. SM turnó la responsabilidad de realizar la investigación a su principal sospechoso, lo cual demostraba el poco interés en descubrir la verdad acerca de los sobornos. El caso se cerró sin mayor investigación y sin dar parte a las autoridades de ambos países.

Ilustración 36. Cronología del caso Supermercado Transnacional



Fecha	Suceso
2003	Una compañía especializada en investigación realizó un trabajo para la empresa, en el que descubrió que ésta había incrementado sistemáticamente sus ventas ayudando a clientes con altos volúmenes a evadir impuestos.
2004	Se ordenó una auditoría interna a los ejecutivos de SM México que había alertado sobre los pagos a gestores.
21 de septiembre de 2005	El denunciante envió un correo a la abogada del corporativo en EE.UU., comunicándole que poseía información sobre irregularidades autorizadas por los más altos mandos de la filial en México. Se reunieron en tres ocasiones.

Fecha	Suceso
15 de noviembre de 2005	El equipo de investigación llegó a la filial en México y se dispuso a revisar la base de datos en busca de descripciones de pagos bajo el concepto “gestoría”. Al final del día encontraron 441 pagos, cada uno contenía un soborno potencial y apenas habían cubierto el año 2003.
Diciembre de 2005	El equipo de investigación escribió un reporte confidencial, mostrando la evidencia que corroboraba lo dicho por el denunciante.
Enero de 2006	El caso llegó a un punto crítico, pues el corporativo evaluaba si aprobaban una investigación que inevitablemente apuntaría al ejecutivo.
1 de febrero de 2006	El ejecutivo presentó su renuncia, pero insistía en la necesidad de expandir la investigación y tratar con igual respeto tanto a la ley mexicana como a la estadounidense.
10 de mayo de 2006	Los ejecutivos en EE.UU. ordenaron al auditor forense que concluyera su reporte y con ello diera fin a la investigación.
Abril de 2012	Un reconocido periódico de EE.UU. publica un artículo del caso, SM no había dado a conocer la información acerca de la investigación realizada.

Detección del fraude

El 21 de septiembre de 2005, el denunciante envió un correo a la abogada del corporativo, comunicándole que poseía información sobre irregularidades autorizadas por los más altos mandos de la filial en México. La abogada atendió el correo del denunciante y contrató a un investigador, abogado experto en investigación, cuyo despacho estaba instalado en la Ciudad de México, para que interrogara al denunciante. Se reunieron en tres ocasiones en octubre de 2005 y a la tercera reunión acudió la abogada del corporativo.

La denuncia anónima se da, en la mayoría de los casos, por personas involucradas en el fraude que se encuentran enojados porque se les deja fuera de las operaciones fraudulentas, o ex empleados de la organización que fueron despedidos por razones injustas o intereses organizacionales. Estas denuncias deben ser investigadas y confirmadas por los investigadores/auditores forenses, hasta acabar con la sospecha de la comisión de un delito.

Valiéndose de la entrevista forense, el abogado investigador obtuvo información acerca de la manera en que la empresa realizaba los sobornos por medio de la contratación de “gestores” que en México son comunes para agilizar trámites burocráticos y cómo eran ocultados por medio de una contabilidad fraudulenta. El denunciante involucraba al presidente del consejo general, al consejo general, al auditor general y al director ejecutivo de bienes raíces de la filial en México. Señalaba que el mayor responsable era el director de operaciones para la empresa SM México. Menciona que dicha compañía se fijó metas de crecimiento muy agresivas para abrir el mayor número de tiendas posibles en un tiempo récord. El abogado era un empleado inconforme que renunció a la compañía en 2004 debido a que consideraba que no apreciaban su trabajo, dada la presión que vivía teniendo que ser parte de la corrupción y tratando con agentes de gobierno corruptos.

Anteriormente en 2003, una empresa especializada en investigación ya había realizado un trabajo para la compañía, en el que descubrió que ésta había incrementado sistemáticamente sus ventas, ayudando a clientes con altos volúmenes a evadir impuestos. Informes de auditoría de la empresa indicaban que se habían ignorado banderas rojas de fraude. También evaluó las unidades de investigación de fraude de SM México y las calificó de ineficaces, encontrando que algunos de los empleados acusados de delitos habían sido promovidos en sus puestos de trabajo.

Asimismo, la empresa contaba con un despacho de abogados expertos para investigar casos de fraude. Al descubrir fraudes realizados a la compañía por altos ejecutivos, realizaron investigaciones exhaustivas llevadas a las últimas consecuencias. Sin embargo, en este caso en el que la empresa realizaba sobornos al gobierno, evitaron realizar investigaciones detalladas y deslindaron la responsabilidad de la investigación a SM México (lugar en donde se estaba cometiendo el fraude) y éstos, en lugar de verificar los permisos, revisaron algunas tiendas e hicieron diversas entrevistas. Este caso es considerado un fraude corporativo de cuello blanco, en donde el soborno y la corrupción se llevan a cabo con las personas de mayor rango de la organización, así como en colusión con el gobierno y empresas externas.

El departamento de investigación de fraude de SM no contaba con el personal suficiente y capacitado para realizar una investigación sobre fraude de esta naturaleza, contaba con menos de 70 empleados, la mayoría de ellos asignados a perseguir pequeños robos e incidentes menores de corrupción en ventas y contaban con tan sólo cuatro personas dedicadas a investigar fraude corporativo, una cifra totalmente inadecuada para una compañía de esa naturaleza. Asimismo, derivado de investigaciones anteriores, se cuestionó la independencia de este departamento.

La investigación de fraude debe ser realizada por personal altamente capacitado, especialista en investigación, ya que fallos en la metodología y en los procedimientos podrían demeritar la investigación realizada.

Curso de la investigación

Por motivo de la denuncia se contrató a un equipo de investigaciones especiales de fraude, dirigidos por un experimentado investigador criminal que había trabajado durante 21 años para el FBI y, en colaboración con un auditor de alto nivel y un grupo de auditores hispanoparlantes, realizarían tal investigación.

La auditoría forense es un trabajo interdisciplinario de profesionales de diversos perfiles como auditores, investigadores, criminalistas y, en este caso, podría incluir abogados y expertos en legislación ambiental, con el objetivo de determinar las violaciones a la ley presuntamente existentes.

El 15 de noviembre de 2005, el equipo de investigación llegó a la filial en México y se dispusieron a revisar la base de datos en busca de descripciones de pagos bajo el concepto “gestoría”. Al final del día habían encontrado 441 pagos, cada uno contenía un soborno potencial y apenas habían cubierto el año 2003.

El denunciante informó que los gestores principales eran dos abogados, cuyos nombres aparecían en cerca de 50% de los pagos por concepto de gestoría y correspondían acerca de \$8.5 millones en pagos; mostraban además que la filial en México pagaba de manera rutinaria decenas de miles de dólares por permiso, se confirmó que ejecutivos de alto nivel estaban al tanto de los pagos.

En 2004 se había ordenado una auditoría interna a los ejecutivos de SM México, la cual había alertado sobre los pagos a gestores; los gestores principales habían recibido millones de dólares para facilitar la autorización de permisos de instalación de nuevas tiendas en todo el país. La auditoría no investigó cómo el dinero había sido utilizado para facilitar los permisos, pero mostró que éstos se habían incrementado de manera rápida, todo ello en concordancia con el crecimiento acelerado de la empresa. La auditoría recomendaba notificar al corporativo en Estados Unidos de América acerca de los pagos, sin embargo, existe evidencia de que la recomendación fue removida por el auditor general de la compañía y, posteriormente, el auditor que realizó la auditoría fue despedido. La información de la auditoría había sido removida al consejero general de SM México, que entre sus observaciones incluía la existencia de “tarjetas de regalo” a funcionarios de gobierno.

La auditoría interna juega un papel importante en la detección de fraude, ya que mediante ésta se pueden detectar indicios de la comisión de delitos. Sin embargo, al pertenecer a la organización, la independencia puede estar comprometida, al tratarse de un fraude de alto nivel. Los auditores internos deben informar, ante órganos competentes, la existencia de delitos y sugerir investigaciones adicionales en caso de que así lo consideren. El auditor interno no está capacitado para realizar investigaciones más profundas, sin embargo, debe brindar evidencia suficiente que permita tomar la decisión de iniciar una investigación. La cadena de custodia de dichas evidencias debe ser protegida durante el proceso de auditoría.

Por último, al repasar los pagos en la base de datos de SM México, los investigadores anotaron que la empresa había realizado grandes contribuciones y “donaciones” directamente a los gobiernos locales en todo México (cerca de \$16 millones de dólares desde 2003). Algunas de las descripciones de pagos indicaban que se trataba de “donaciones” para la expedición de una licencia.

Las técnicas de investigación forense están encaminadas a detectar información sospechosa, por medio del análisis numérico o de palabras clave. En este caso, la búsqueda de palabras como “gestoría” o “donaciones” en los conceptos de los registros contables, puede dar lugar a la identificación de patrones anormales de comportamiento en pagos realizados por la organización. El análisis de información de diversas fuentes, montos, comportamiento de ejecutivos y alta rotación de personal, permite al auditor llegar a conclusiones válidas acerca de posible comisión de fraude.

Cuando el equipo de investigación estaba preparado para entrevistar a los ejecutivos de SM México, el primer objetivo era el principal sospechoso, quien antes de trabajar para la compañía en 2004, se había desempeñado como abogado en una importante firma de México; el denunciante había identificado su participación directa en el esquema de sobornos, pues seguía las instrucciones del director ejecutivo del corporativo en Estados Unidos de América para ejecutar pagos. El principal sospechoso no quiso comentar nada al respecto y el viernes SM anunció su reasignación y que ya no formaba parte del consejo general de la empresa.

Los investigadores pidieron realizar una entrevista al principal sospechoso y su personal, pero recibieron una respuesta negativa; al presentar una queja con altos ejecutivos de SM, accedieron y postularon como principal sospechoso al denunciante, fue entonces cuando SM pidió a una agencia de investigación externa, que investigara el beneficio que estas transacciones podían traer al denunciante. Los ejecutivos aseguraron que la agencia descubrió que la esposa del denunciante era socia del bufete de uno de los gestores y que debido a que no había informado a SM sobre el particular, éste había sido despedido.

El principal sospechoso argumentó que los pagos a gestores habían sido en todo caso una estrategia del denunciante para defraudar a SM México y que, probablemente, éste y los gestores se habían quedado con el dinero de los sobornos.

Los sobornos no hubieran podido pagarse si el dinero hubiera sido robado en primera instancia; este argumento fue suficiente para que SM diera carpetazo a la investigación, a pesar de que, según consta en su informe, los investigadores mostraban escepticismo. Si era cierto el relato del principal sospechoso, no explicaba por qué los ejecutivos de SM México habían autorizado pagos a gestores, tampoco decía por qué habían realizado donativos para obtener permisos, ni por qué alteraron las auditorías para ocultar al corporativo lo que estaba sucediendo.

Los documentos contradecían la mayoría de las afirmaciones de los ejecutivos, pues según los archivos de la compañía, el denunciante no había sido despedido, sino que había renunciado con beneficios de liquidación y un bono de \$25 mil dólares. Después de su regreso al corporativo en Estados Unidos de América en diciembre de 2005, el equipo de investigación escribió un reporte confidencial, mostrando la evidencia que corroboraba lo dicho por el denunciante: los cientos de pagos a gestores, los códigos misteriosos, las auditorías alteradas, las respuestas evasivas de los ejecutivos mexicanos, las donaciones para obtener permisos, la evidencia de que al día de hoy la empresa utilizaba gestores, teniendo como conclusión: “Existe sospecha razonable para creer que han sido violadas leyes mexicanas y estadounidenses”. No hay “explicación plausible” que justifique los millones de dólares que se gasta la empresa en pagos a gestores”.

Se propuso una investigación sobre los dos gestores, misma que no se había querido iniciar por miedo a su seguridad mientras el líder estaba en México. Se solicitó que SM contratara a investigadores privados para entrevistar y monitorear a ambos gestores, además de hacer lo mismo a los altos ejecutivos y, en especial, al director del corporativo en Estados Unidos de América sobre su papel en los pagos de gestoría.

En enero de 2006 el caso llegó a un punto crítico, pues el corporativo evaluaba si aprobaban una investigación que inevitablemente apuntaría al ejecutivo estrella del cual se afirmaba públicamente, podría llegar a ser el sucesor de Scott, entonces director ejecutivo de la empresa y cuando su código ético señalaba “nunca encubras o ignores un problema ético”. Algunos comentaban que si hubiera ocurrido en Estados Unidos de América, la cosa sería distinta, pero calificaban a México como un país en donde el soborno se encuentra incrustado en la cultura de los negocios y que por ello no ameritaba la misma reacción. El primero de febrero de 2006 y en pleno debate, la abogada del corporativo en Estados Unidos de América presentó su renuncia, insistiendo en uno de sus últimos memos sobre la necesidad de expandir la investigación y tratar con igual respeto tanto a la ley mexicana como a la estadounidense; advirtió que los ejecutivos no debían inmiscuirse en la investigación.

El principal riesgo en las organizaciones es el incumplimiento de leyes y regulaciones. Las organizaciones con presencia internacional deben dar cumplimiento a las normativas internacionales, sobre todo en las localidades donde se encuentran en funcionamiento. Es importante durante el curso de una investigación, observar el cumplimiento de los mismos y la cultura ética que existe en general, así como la existencia de un marco de control y riesgos antifraude.

Por su parte, SM tomó las medidas de realizar una reunión vía videoconferencia para hablar sobre el caso con los responsables en México y como respuesta emitió un nuevo protocolo para investigar fraudes, así como deslindó la responsabilidad de investigar este caso al principal sospechoso, quien, como es de esperar, cerró el caso en pocas semanas y con una nula investigación adicional. Su reporte concluía: “No existe evidencia clara o indicación de sobornos pagados a autoridades gubernamentales mexicanas con el propósito de asegurar licencias o permisos”.

En su reporte incluyó que ninguno de sus colaboradores informaba haber pagado sobornos, ni mucho menos que él mismo había estado involucrado; por el contrario, inculpaba al denunciante por haber defraudado a la compañía, engañándola y beneficiándose de los pagos a gestores; todo esto sin brindar pruebas suficientes que lo respaldara; menciona haber consultado a un experto en fraude, quien argumenta que la conducta del denunciante es la típica de un defraudador. Asimismo, menciona haber realizado un análisis estadístico en el que muestra que SM había obtenido permisos con mayor celeridad desde que el denunciante abandonó la compañía, siendo difícil de comprobar la validez de su análisis.

El reporte fue enviado al corporativo en Estados Unidos de América, y se dictaminó como deficiente, ya que era incongruente que el denunciante hubiera cometido un fraude por 10 millones de dólares, esto fuera descubierto y no se tomaran acciones legales al respecto en su momento; no obstante, el 10 de mayo de 2006, los ejecutivos del corporativo en Estados Unidos de América ordenaron al principal sospechoso que “concluyera su reporte y con ello diera fin a la investigación”.

La metodología de auditoría forense tiene un enfoque sistemático enfocado en la obtención de evidencia de relevancia legal para probar la existencia de un presunto delito. Los sospechosos no deben participar en la investigación y el proceso debe seguirse de manera confidencial y objetiva, con el objetivo de evitar dar aviso a los implicados y éstos oculten o destruyan evidencia relevante para el caso. Asimismo, las organizaciones son responsables de informar a las autoridades competentes la existencia de delitos dentro o fuera de la organización. El involucramiento del sector público y privado requiere la intervención de distintos órganos reguladores para la determinación de responsabilidades en caso de que se probara la comisión de violaciones a la ley.

Para prevenir y detectar fraude en organizaciones del sector público, la auditoría forense, tema de estudio del presente trabajo, tiene como rol principal el de facilitar la prevención, detección e investigación del crimen económico. Esto incluye los siguientes aspectos:

1. Creación de un programa de prevención contra el fraude y una estrategia al respecto para cada institución pública.
2. Revisión del sistema legal para tener claro qué conductas constituyen un daño a las normas y leyes.
3. Desarrollo de unas políticas y normas necesarias, incluyendo un modelo apropiado de riesgos para auditorías y otros propósitos.

Asimismo, en el sector privado, el rol de la auditoría forense está en la prevención de actos que atenten contra la equidad, en las transacciones que involucren el interés público; las entidades que han adoptado este tipo de servicios en gran medida son las que se encuentran en el sector financiero, dado que allí existe un alto grado de vulnerabilidad al sistema legal, cuando se intenta blanquear dinero, escondiendo negocios que se generan en comercio de armas y narcotráfico, así como la corrupción en general. Ambos (el sector público y privado) están íntimamente relacionados en la mayoría de los casos de corrupción que se detectan. Por tal motivo, ha sido primordial que la legislación en México y otros países tengan un enfoque integral en cuanto a sus marcos de actuación, de manera que contemplen mecanismos adecuados para la denuncia, investigación y proceso legal adecuados de presuntos incumplimientos e irregularidades, así como sanciones adecuadas que permitan a la sociedad mantener la confianza en las instituciones.

En México, el Sistema Nacional Anticorrupción establece un marco legal de nueva creación, que propone una estructura de funcionamiento coordinada entre diversas organizaciones del sector público y que tiene como objetivo erradicar la corrupción en el gobierno y sus relaciones con el sector privado.

2.2.2 Caso de la empresa Ingeniería Marina

2.2.2.1 Descripción de la empresa

La empresa Ingeniería Marina fue fundada en 1968 para proveer servicios a una compañía petrolera en México; se especializa en ingeniería geofísica marina, buceo de saturación, operación de vehículos sumergibles manejados a control remoto, mantenimiento a estructuras marinas y construcción de ductos submarinos.

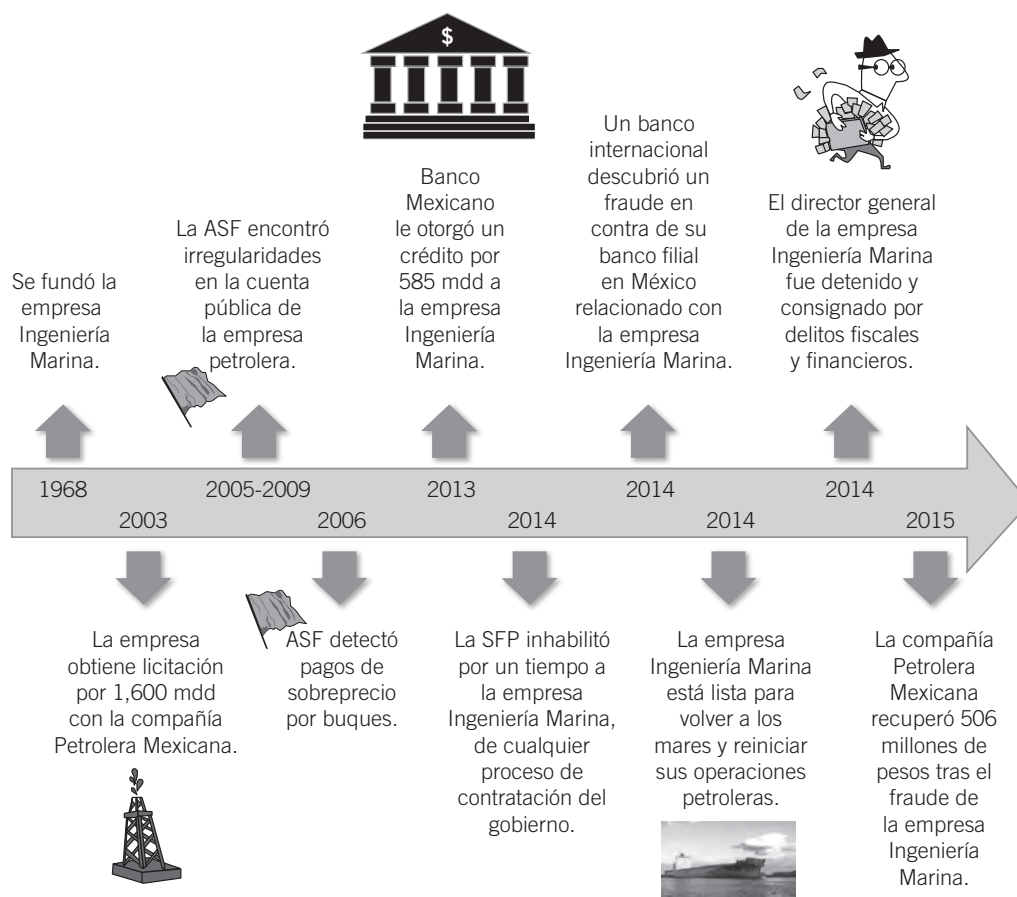
En el año 2013 contaba con más de 4,500 trabajadores y su flota está integrada por 38 embarcaciones que representan 70,862 toneladas de arqueo bruto y se encuentran en proceso de construcción ocho embarcaciones diseñadas para operar en las diferentes actividades de la industria petrolera; los activos de la empresa Ingeniería Marina cuenta con una flota y equipos con un valor de 16,700 millones de pesos (1,243 millones de dólares), según reportes del 2012.

Cronología

La empresa Ingeniería Marina que le provee servicios a la compañía Petrolera Mexicana, se vio involucrada en un fraude de 400 millones de dólares cuando solicitó un préstamo a Banco Mexicano y puso como garantía supuestos pagos que esperaba de la empresa petrolera.

Un banco internacional que es filial de Banco Mexicano, en conjunto con la empresa petrolera, comenzaron a revisar la exposición del crédito que Banco Mexicano le había otorgado a la empresa Ingeniería Marina y de su programa de financiamiento de los últimos años. En consecuencia, en 2014 se descubrió un fraude en contra de Banco Mexicano, relacionado con la firma de servicios petroleros de la empresa Ingeniería Marina.

Ilustración 37. Cronología del caso de la empresa Ingeniería Marina



Fuente: Elaborado por el autor.



Fecha	Suceso
2003	La empresa Ingeniería Marina obtiene una licitación por 1,600 mdd con la compañía Petrolera Mexicana.
2005, 2006, 2007, 2008 y 2009	En las revisiones de la cuenta pública de la empresa petrolera, la Auditoría Superior de la Federación (ASF) encontró serias irregularidades en la forma de operar de la compañía.
2006	Se detectaron pagos de sobreprecio por la renta de buques; el órgano fiscalizador presentó una denuncia penal ante la PGR el 6 de diciembre de 2007.
6 de diciembre de 2007	La Cámara de Diputados creó una comisión legislativa para darle seguimiento al pliego de observaciones. Un año después, el Ministerio Público Federal determinó el no ejercicio de la acción penal.
31 de diciembre de 2013	Banco Mexicano otorga un crédito por 585 mdd a la empresa Ingeniería Marina.
15 de enero de 2014	La empresa Ingeniería Marina incumple pago de 19 mdd a Banco Mexicano por concepto de intereses.
11 de febrero de 2014	La SFP inhabilitó por un año, nueve meses y 12 días a la empresa Ingeniería Marina, de cualquier proceso de contratación del gobierno, luego que la compañía Petrolera Mexicana encontró, en una revisión interna, irregularidades en contratos con la firma como fianzas inferiores a las debidas.
20 de febrero de 2014	La empresa Ingeniería Marina es investigada por fraude al registrar Banco Mexicano pérdidas por 400 mdd.
28 de febrero de 2014	Una empresa de servicios financieros descubrió un fraude en contra de su filial mexicana, relacionado con la firma de servicios petroleros, por lo que recortó su ganancia neta de 2013 en 235 millones de dólares.
2 de marzo de 2014	Según datos de la PGR, la firma naviera alteró los convenios que suscribía con la empresa Petrolera Mexicana, con base en los cuales disfrazó sus niveles de operación y ganancias, es decir, falsificó más de 160 documentos de la paraestatal para obtener financiamiento de Banco Mexicano.
4 de marzo de 2014	Banco Mexicano registró un impacto negativo en su utilidad neta por 3 mil 177 millones de pesos, derivado del fraude cometido por la empresa Ingeniería Marina, lo que representa alrededor de 2% del capital contable del grupo.
22 de marzo de 2014	El dueño de la empresa Ingeniería Marina fue detenido por agentes ministeriales en el Distrito Federal.
10 de junio de 2014	La Procuraduría Fiscal denunció ante la PGR a 10 directivos y empleados de Banco Mexicano, presuntamente por haber consentido una serie de operaciones fraudulentas en favor de la empresa Ingeniería Marina.
11 de junio de 2014	El director general de la empresa Ingeniería Marina acusó, ante la PGR, a uno de sus socios de ser el único responsable.
25 de agosto de 2014	La empresa Ingeniería Marina está lista para volver a los mares y reiniciar sus operaciones petroleras, después de una serie de negociaciones con sus acreedores.
22 de octubre de 2014	El titular de la PGR informó que el accionista mayoritario de la empresa Ingeniería Marina fue detenido y consignado por delitos fiscales y financieros.
22 de marzo de 2015	La empresa Ingeniería Marina podrá volver a rentar sus embarcaciones, a fin de que pueda seguir operando y logre ingresos para saldar sus deudas.
28 de abril de 2015	La empresa Petrolera Mexicana recuperó 506 millones de pesos después del fraude.

Tipos de fraude

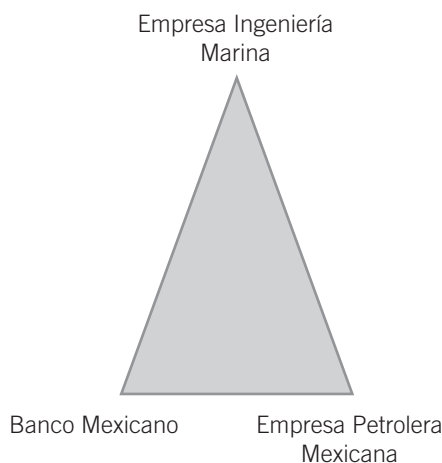
- Fraude bancario.
- Falsificación de documentos.

Involucrados en el fraude

- Fundador de la empresa Ingeniería Marina.
- Director de la empresa Ingeniería Marina.
- Un accionista de la empresa Ingeniería Marina.
- Empresa Petrolera Mexicana.
- Banco Mexicano.

Impacto del fraude

La empresa Ingeniería Marina cometió un presunto fraude en contra de Banco Mexicano por la cantidad de 400 millones de dólares, derivados de la cesión de derechos de cobro provenientes de 112 contratos celebrados entre la compañía y Petrolera Mexicana por un total de 585 millones de dólares, de los cuales únicamente se encontraban respaldados por la paraestatal 185 millones de dólares (Comisión especial para la atención y seguimiento al caso de la empresa Ingeniería Marina).



2.2.3 Caso Lavado de dinero: Cyber criminals-dinero digital

Tipo de fraude

- Delito cibernético.
- Robo de identidad.
- Lavado de dinero.
- Tráfico de datos de tarjetas de crédito.

Cronología

A principios de 2005 en la Oficina del Fiscal de Distrito del Condado de Nueva York, se recibió una queja que alegaba que la tarjeta de crédito de una víctima había sido utilizada sin autorización en un minorista en línea para enviar mercancía a una dirección de Manhattan.

Supuesto monto del valor total de los contratos entre las empresas Petrolera Mexicana e Ingeniería Marina hasta el 31 de diciembre de 2013:	585 millones de dólares
Supuesto monto respaldado por la empresa Petrolera Mexicana:	185 millones de dólares
Supuesto monto del fraude:	400 millones de dólares

Los investigadores siguieron el rastro del dinero de los participantes en línea en este robo, y se encontraron con un cambiador de moneda digital en Manhattan llamado International Express.

Por presiones externas, International Express estaba actuando como un cambiador de cheques y transmisor de dinero para una clientela de habla rusa basada en Europa del Este, pero ganando dinero dentro de los EE.UU. Sin embargo, la compañía no tenía licencia del Estado para cobrar cheques o transferir dinero. Se obtuvo una acusación contra ellos por estos crímenes en 2006. Los análisis de las computadoras y los registros tomados de la compañía revelaron que muchos de sus clientes de cambio de moneda digital eran ciberdelincuentes de élite y ladrones de identidad, y la compañía a sabiendas estaba facilitando sus crímenes y lavando sus ganancias ilegales.

En última instancia, International Express y algunos de sus clientes fueron acusados nuevamente por una variedad de cargos, incluyendo el lavado de dinero (de moneda digital) y los cargos relacionados con el tráfico de datos de tarjetas de crédito robadas y otra información personal robada.

Total desconocimiento de los clientes y su importancia

Investigando el informe inicial de fraude de tarjeta de crédito, el minorista en línea dijo que otros pedidos fraudulentos fueron colocados con números de tarjetas de crédito adicionales para ser enviados a la misma dirección de Manhattan. Así que se comprobó con otros comerciantes en línea y rápidamente se identificaron cerca de 100 órdenes de fraude con esa misma dirección. Debemos reconocer la naturaleza global del lavado de dinero en moneda digital.

Las órdenes de fraude no fueron enviadas a un ladrón de identidad maestro sino simplemente a un participante en un plan de reventa —una variante en el esquema de reenvío—. En un esquema de reenvío, un ciberdelincuente recluta una “gota” (por ejemplo, una ventosa) para recibir inadvertidamente mercancía comprada con información de cuenta de tarjeta de crédito robada y luego volver a enviarla a una dirección controlada por el cibercriminal, normalmente en otro país. Aquí, el individuo en la dirección de Manhattan que recibía los envíos fraudulentamente comprados, los revendía en línea para obtener ganancias.

El revendedor estaba utilizando E-gold moneda digital para pagar el fraude; en ese momento no se sabía casi nada sobre E-gold, la moneda digital, el cibercrimen, las direcciones de Internet Protocolo (IP) y el lavado de dinero. E-gold era popular entre los criminales cibernéticos, los ladrones de identidad, los pedófilos, los intrigantes de Ponzi y los que creían en el “estándar de oro” y no en las monedas respaldadas por el gobierno. E-gold también estuvo a la vanguardia de un movimiento de divisas digitales que se ha vuelto más corriente.

Cerca de \$4 millones del negocio de International Express durante cuatro años consistió en recibir y depositar cheques en nombre de sus clientes y transmitir esos fondos en el extranjero. Sin embargo, no tenían licencia para hacerlo, por lo que violaron las leyes bancarias de Nueva York. Son las pruebas de la acusación No. 1.

Las leyes de transmisión de dinero son los primeros pasos para tratar de mantener limpios nuestros sistemas financieros y evitar que se conviertan en conductos para la actividad ilícita y proceda. Los individuos y las compañías que mueven dinero se supone deben ser regulados y deben seguir los procedimientos contra el lavado de dinero que incluyen protocolos del conocer-su-cliente y divulgar de la actividad sospechosa al gobierno.

Las transgresiones de la empresa demostraron por qué esas leyes son importantes, la compañía no tomó medidas para conocer a sus clientes, sino que les permitió cobrar cheques hechos a nombres obviamente ficticios. A continuación, International Express remite el dinero al cliente como él/ella eligió a las cuentas en el extranjero o mediante la moneda digital o Western Unión. International Express utilizó este método de pago de baja tecnología para permitir que los que viven en el extranjero recibieran anónimamente fondos procesados por medio del sistema bancario de Estados Unidos. La empresa también ofreció una variedad de otros servicios, muchos de los cuales diseñó para permitir a los clientes anónimamente transferir o gastar fondos. La compañía emitió órdenes de pago, facilitó pagos por medio de otros transmisores de dinero y revendió tarjetas de regalo.

Los servicios de International Express eran costosos para los servicios financieros tradicionales, tales como el cobro de cheques, giros postales, tarjetas de regalo o cambio digital de divisas. Pero los clientes estaban dispuestos a pagar una alta prima por el anonimato.

Así que cuando se está evaluando una base de clientes, revisa los costos de los servicios y la facilidad de uso. Muchos defensores dicen que las empresas ahorran dinero y tiempo cuando usan monedas digitales en comparación con los bancos tradicionales o Western Unión o MoneyGram. Son correctos hasta cierto punto, pero debe evaluar el costo total del uso de una moneda digital, ya que cuesta dinero para cobrar y sacar dinero. Por ejemplo, los clientes pagaron aproximadamente una comisión de 5% para convertir dinero en efectivo (giros postales) en moneda digital, que luego utilizaron para pagar a criminales extranjeros. En el otro extremo, los delincuentes extranjeros pagaban una comisión (a veces a otros intercambiadores) para convertir una moneda digital en otra o para convertirla en moneda tradicional.

Movimientos de la moneda digital fuera del país

Pasó más de un año analizando los registros de esta empresa para entender completamente su negocio de cambio digital de divisas y para demostrar que era un centro financiero del tráfico de datos cibernéticos. En cuatro años, \$35 millones en moneda digital fluyeron por medio de la corporación. Si alguno de esos fondos era legítimo, probablemente fue por puro accidente.

El lavado de dinero y delitos relacionados se identificaron alrededor de \$2 millones como el producto de la actividad criminal.

La capacitación y los procedimientos contra el lavado de dinero se centran a menudo en los riesgos que plantean las transacciones en efectivo, pero probablemente la industria no se ha dado cuenta plenamente de la amenaza del blanqueo de dinero en moneda digital. El efectivo es una gran herramienta para las transacciones criminales en persona, como la venta de drogas. Como la serie de televisión “Breaking Bad” ilustrando a los traficantes de drogas con éxito, rápidamente se dan cuenta que tienen que resolver el problema de cómo utilizar su dinero sin violar las regulaciones financieras y sin levantar sospechas sobre su fuente. Dicho capital no pueden usarlo para comprar una casa, un barco o un coche sin arriesgarse a llamar la atención. Deben idear métodos y planes para obtener dinero en efectivo en el sistema financiero sin necesidad de detección para que puedan comprar las cosas que quieran.

El blanqueo de dinero en moneda digital tiene un flujo ligeramente diferente. Los delincuentes acumulan sus beneficios ilícitos mediante la ciberdelincuencia, pero todavía tienen que ocultarlos, deben seguir varios pasos para convertir el dinero en fondos lavados que se pueden gastar. Con la aparición y popularidad del bitcoin, los ciberfraudadores tienen puntos de venta más fáciles por medio de los cuales pueden lavar sus productos criminales. Desde un punto de vista crítico, ya no es esencial que primero conviertan sus fondos ilícitos a moneda fiduciaria tradicional antes de comprar los productos que desean.

Si queremos entender el lavado de dinero en moneda digital debemos reconocer su naturaleza global, su semejanza con otros modelos de comercio internacional y su interconexión con el sistema financiero convencional. Lo más importante es que los cibercriminales fuera de los Estados Unidos utilizan regularmente métodos como éstos para obtener fondos ilícitos generados por victimizar a los residentes de los Estados Unidos fuera del país.

La segunda acusación: 18 acusados de participar en el programa de lavado de dinero y tráfico de datos de International Express. Cinco de estos acusados eran cibercriminales internacionales bien conocidos que residían cómodamente en el extranjero mientras se robaban información de víctimas estadounidenses. Muchas de las fuerzas de seguridad de Estados Unidos y las comunidades financieras dudan de la eficacia de perseguir a los ciberdelincuentes que actúan desde fuera de nuestras fronteras, las autoridades tuvieron notable éxito acusando y extraditando a los acusados internacionales en este caso. Dos acusados (ciudadanos rusos y moldavos) fueron detenidos en la República Checa, extraditados a Nueva York y finalmente se declararon culpables en 2010.

Otro acusado, el ucraniano, fue detenido mientras estaba de vacaciones en Grecia, extraditado a Nueva York y condenado después del juicio en 2013. Fue uno de los proveedores más prolíficos del mundo de datos de tarjetas de crédito robadas en el mercado negro cibernético. En su esquema de triangulación, reclutaron socios para anunciar

mercancía para la venta en línea. Una vez que un comprador de buena fe pagó la mercancía, los ciberdelincuentes utilizaron información de tarjeta de crédito robada para ordenar la mercancía de un sitio de comercio electrónico y enviarla directamente al comprador.

Uno de los acusados internacionales de este caso, sigue siendo un fugitivo en los cargos de Int. Express y una posterior acusación federal. Vendía datos de tarjetas de crédito robadas y falsificaba identificaciones (como pasaportes) en línea. También sigue siendo un fugitivo en los cargos de Int. Express y una posterior acusación federal, mientras lavaba fondos mediante ésta, aprendía el comercio del delito cibernético y se convirtió en experto. Como demostró la posterior acusación federal, él era un “hacker” de élite capaz de cibercrimen muy sofisticado.

Las transacciones básicas entre los ciberdelincuentes y los ladrones de identidad y cómo se comunican éstos, se pagan entre sí y trafican datos robados. Al final, se trata de ganancias y esta forma de delincuencia es una ocupación muy rentable; también requiere inteligencia y paciencia, habilidades que los ladrones de identidad y los ciberdelincuentes desarrollan y dominan durante años por medio del estudio y la práctica. Aunque los delincuentes estudian cuidadosamente formas de anonimizar a sí mismos y evadir la detección de la aplicación de la ley, pudimos perforar su velo de anonimato en este caso. El proceso de examen del fraude fue una revisión exhaustiva de la evidencia, incluyendo registros financieros y correos electrónicos confiscados con las órdenes de registro en Kiev, Ucrania; Manhattan y Nueva Jersey y en publicaciones en la web, documentos en papel, registros financieros, datos dentro de teléfonos celulares y computadoras y mensajes de chat.

El jurado recabó información y por dos meses trabajó en testimonios y pruebas, incluyendo más de 50 testigos y una montaña de registros en papel, datos electrónicos y otras pruebas. Derribamos a International Express sólo debido a una asociación con el Servicio Secreto de los Estados Unidos (que había pasado años desarrollando conocimientos especializados en la lucha contra la ciberdelincuencia); la inversión que hicieron los supervisores, el equipo de investigación y el arduo trabajo de analistas, investigadores, agentes especiales y muchos otros en la aplicación de la ley y los sectores financieros. Fue un verdadero esfuerzo de equipo.

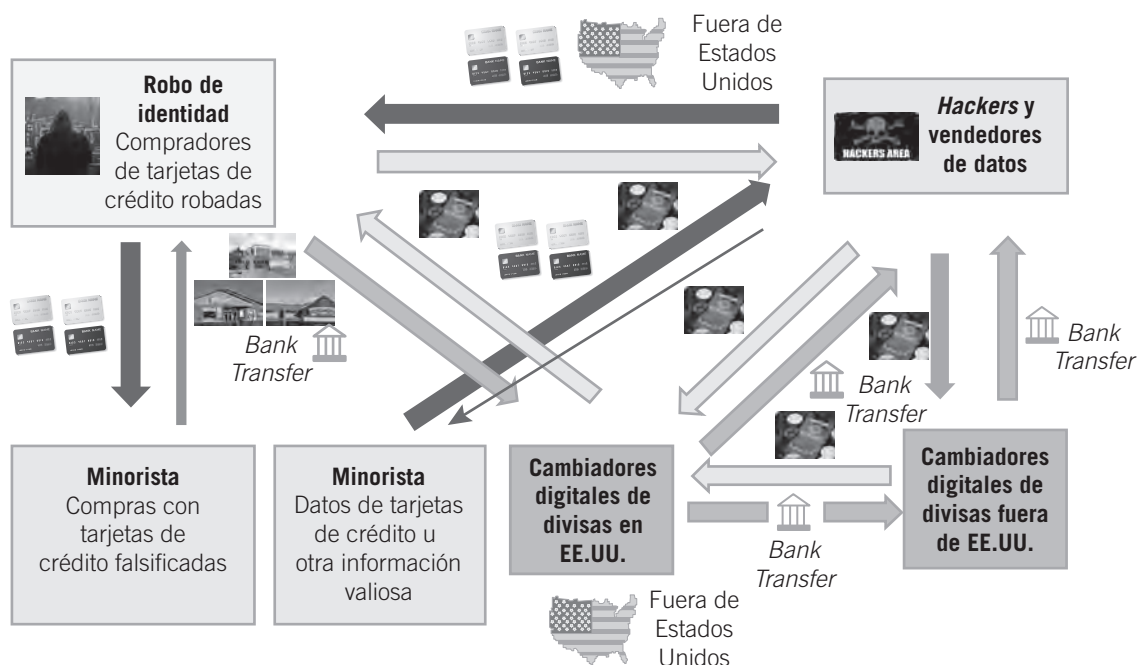
Los sectores de justicia penal en todo el mundo están tratando de combatir el delito cibernético y el robo de identidad, que han crecido hasta proporciones épicas con niveles de éxito variables. El robo de PII (Personally Identifiable Information-Información de identidad) y el uso de monedas digitales han sido una parte de la economía del delito cibernético desde principios de los años 2000.

Los ciberdelincuentes están bombardeando individuos y corporaciones con ingeniosos tipos de ataques; los gobiernos deben desempeñar papeles más importantes para ayudar a proteger la información personal de sus ciudadanos y aprehender a los responsables de comprometerla. Las empresas también necesitan proteger sus datos, clientes y empleados. La ciberseguridad es importante, pero la solución a este problema no puede ser la transformación de las corporaciones en fortalezas cibernéticas que son impermeables a los ataques repetidos y los empleados a los expertos en delincuencia cibernética, idealmente alertas a variaciones interminables de estafas y esquemas de ingeniería social.

Las autoridades tienen que mejorar en la aprehensión de más ciberdelincuentes, disuadiendo así aquellos que se enfrentan a un riesgo mínimo de aprehensión y sanciones mediante la inversión en auditores forenses. Los fiscales, investigadores, analistas y agentes de la cibercriminalidad tardan años en desarrollarse, al igual que los casos.

Las instituciones financieras también deben mejorar en la prevención y detección del cibercrimen porque son los principales conductos por medio de los cuales se generan y se transfieren beneficios ilícitos a nivel internacional para ser entregados a los ciberdelincuentes. Las instituciones financieras no pueden basarse simplemente en las casillas de verificación de “normas mínimas” de los reglamentos o contratos de titular de cuenta para la debida diligencia para prevenir el fraude, el robo y el lavado de dinero. Los bancos tienen que encontrar mejores maneras de asegurarse, de que los cables internacionales no son simplemente agujeros negros por medio de los cuales nada puede ser recuperado. Deben mirar el problema de manera holística e intentar combatirlo. Ahora estamos tratando con nuevos ladrones, monedas digitales y sitios web; sin embargo, el problema persiste y las soluciones son urgentemente necesarias para poder combatirlo efectivamente.

Ilustración 38. Flujo de moneda digital y robo de información



Fuente: Elaborado por el autor.

2.2.4 Caso de la empresa en óptica e imagen

Descripción de la empresa

Se fundó el 12 de octubre de 1919 con una meta, crear el primer microscopio en Japón, lo cual fue logrado por la compañía al año siguiente de haberse consolidado la empresa; su sede se encuentra en Tokio, Japón. La compañía es una corporación global con extensos recursos en investigación y desarrollo, y con una amplia oferta de productos e instalaciones en todo el mundo. En 1935 se abrió una instalación de investigación óptica de primera categoría, dedicada a crear las lentes más refinadas para cámaras. Desde la primera gastrocámara mundial en 1950 hasta ser los pioneros en el desarrollo de cámaras compactas SLR y las primeras grabadoras microcassette del mundo; la empresa japonesa ha continuado creando exitosas respuestas para cubrir las necesidades del mercado alrededor del mundo. En 2003, el nombre de la empresa fue cambiado con el que hoy en día aparece en la Bolsa de Tokio y en sus cuentas correspondientes al ejercicio finalizado el 31 de marzo de 2011, las ventas netas consolidadas fueron de US\$10.6 millones en el año; la compañía japonesa cuenta con aproximadamente 40,000 empleados alrededor del mundo. Durante la década de 1980, muchas compañías japonesas se basaban en las inversiones para reforzar la disminución de los beneficios, particularmente en sus exportaciones que habían sido erosionadas por un yen fuerte. El presidente de la empresa de 1984 a 1993 admitió, en 1986, en un periódico que: "Cuando el negocio principal está luchando, tenemos que ganar a través de zaitech" (es decir, la ingeniería financiera). La empresa japonesa invirtió en cosas arriesgadas para aumentar sus ganancias. En 1991, la compañía tuvo que asumir pérdidas de ¥2.1 billones en el valor de sus inversiones después de que la inversión bonanza terminara. En junio de 1998, la empresa japonesa fue objeto de rumores de mercado que había sufrido pérdidas considerables en el comercio, lo que causó que sus acciones se desplomaran en 11%. Los rumores fueron negados rotundamente por la compañía que, posteriormente, anunció beneficios récord.

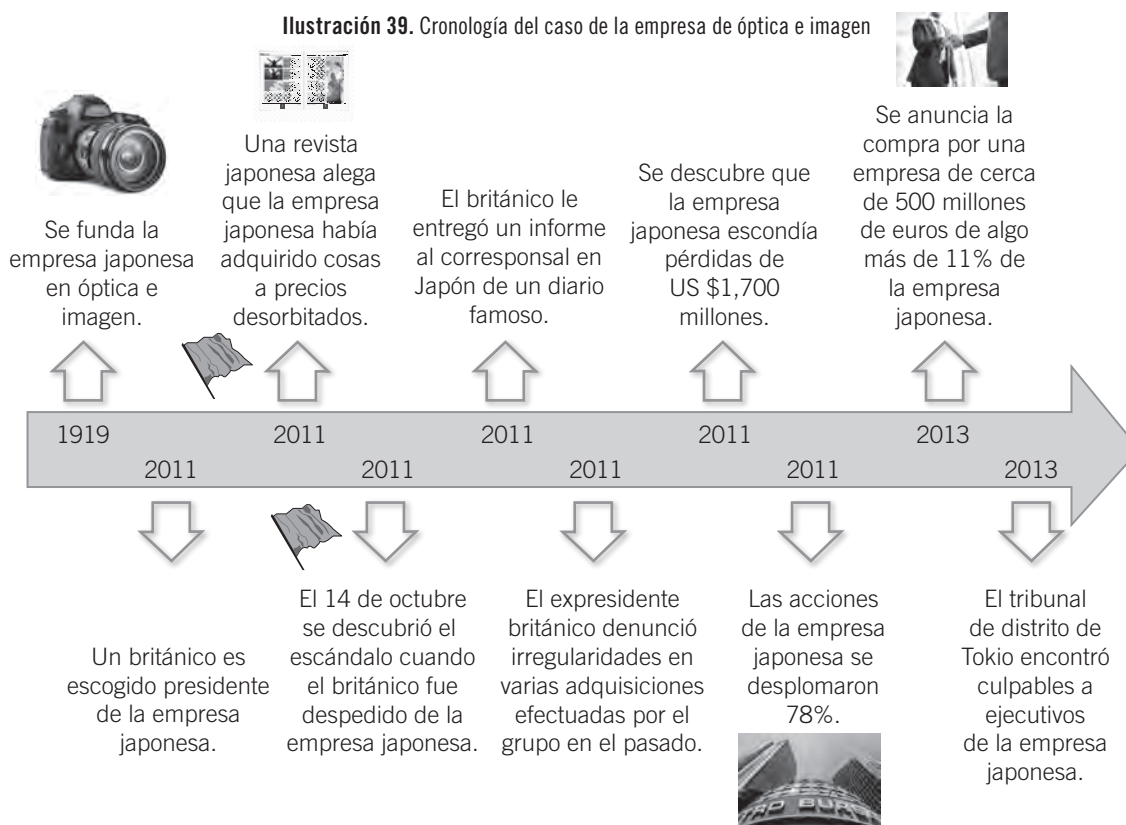
Cronología

El 14 de octubre de 2011, el presidente ejecutivo británico fue expulsado repentinamente de la empresa. Éste había sido presidente de la compañía durante seis meses y dos semanas; los pagos irregulares para adquisiciones habían dado lugar a muy significativos cargos por deterioro de activos en las cuentas de la compañía, y esto fue

expuesto en un artículo en la revista financiera japonesa y ya habían llegado a la atención del expresidente de la empresa japonesa. La prensa japonesa especula sobre una conexión de la compañía con el crimen organizado, a pesar de las negativas de la empresa japonesa; el asunto se agravó rápidamente en un escándalo de corrupción corporativa sobre la ocultación de más de US\$1,500 millones de pérdidas de inversión y otros cargos dudosos que se remontan a finales de 1980 y se sospecha que al igual se realizaron pagos encubiertos a organizaciones criminales. En 2011, la empresa admitió que la práctica de la contabilidad de la compañía era “inadecuada” y que el dinero había sido utilizado para cubrir las pérdidas en las inversiones que datan de la década de 1990.

Para el año 2012 el escándalo se había convertido en uno de los más grandes y de más larga vida de pérdidas financieras de la historia corporativa de Japón; se detuvieron 11 personas entre las que están: pasados y presentes directivos, auditores y banqueros de la empresa japonesa de óptica por presuntas actividades delictivas o encubrimiento.

Ilustración 39. Cronología del caso de la empresa de óptica e imagen



Fecha	Suceso
12 de octubre de 1919	Se funda la empresa japonesa de óptica e imagen.
1 de abril de 2011	El británico es nombrado presidente de la empresa japonesa.
29 de julio de 2011	Una revista japonesa alega que la empresa japonesa había adquirido empresas a precios desorbitados.
14 de octubre de 2011	Se destapó el escándalo cuando se produjo la destitución del entonces presidente de la empresa.
2011	El expresidente de la empresa le entregó un informe al corresponsal en Japón de un famoso periódico.
2011	El expresidente de la empresa japonesa denunció irregularidades en varias adquisiciones efectuadas por el grupo en el pasado.

Fecha	Suceso
8 de noviembre de 2011	La empresa japonesa admitió que la práctica de la contabilidad de la compañía era “inadecuada” y que el dinero había sido utilizado para cubrir las pérdidas en las inversiones que datan de la década de 1990.
14 de noviembre de 2011	Las acciones de la empresa japonesa habían caído 78% desde el 13 de octubre del mismo año, cuando el escándalo emergió.
2012	El escándalo se había convertido en uno de los escándalos financieros más grandes de la historia corporativa de Japón.
Entre abril y septiembre de 2012	El fabricante nipón ganó entre abril y septiembre 8.015 millones de yenes (algo más de 79 millones de euros). Tuvo un incremento de 14.2%.
Junio de 2013	La empresa japonesa presentó un plan de reestructuración a mediano plazo, por el que reducirá hasta 2014 unos 2,700 empleos, cerca de 7% de su plantilla.
Septiembre de 2013	Una empresa anunció la compra por cerca de 500 millones de euros por 11% de la empresa japonesa.
2013	El Tribunal de Distrito de Tokio encontró culpables a algunos accionistas de la empresa japonesa.

Fuente: Elaborado por el autor.

Banderas rojas

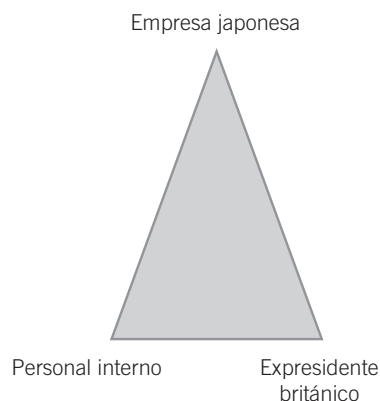
Durante un viaje de trabajo a Europa, el británico expresidente de la empresa japonesa recibió la traducción de un artículo publicado por una revista japonesa de negocios; en él se alega que la empresa japonesa había realizado varias adquisiciones a precios desorbitados en los años precedentes, pagando grandes sumas por empresas casi sin negocio y elevadas comisiones a asesores cuasi desconocidos.

El británico expresidente, al comenzar a trabajar como presidente de la empresa japonesa, tuvo funciones muy limitadas. Éste, después de ver el artículo de la revista de negocios japonesa, habló con dos de sus colegas japoneses, en los cuales confiaba mucho. Éste le preguntó a éstos si habían visto la revista, por lo que contestaron que sí, pero que se habían dado instrucciones por parte de una persona para no comentarle nada a éste.

Involucrados en el fraude

- El expresidente.
- El exvicepresidente ejecutivo.
- El exauditor permanente de la empresa.

Impacto del fraude



La empresa japonesa admitió haber usado una serie de adquisiciones para ocultar fuertes pérdidas. La firma con sede en Tokio ha sido golpeada por el escándalo de un pago de 687 millones de dólares por asesoría financiera y gastos de adquisición de empresas con poca o nula relevancia para sus negocios. El fraude financiero supuso un revés para el grupo, que vio como sus acciones perdían casi la mitad de su valor en la bolsa; el 14 de noviembre de 2011 se informó que las acciones de la empresa japonesa habían caído 78% desde el 13 de octubre del mismo año, cuando el escándalo emergió. Desde el despido del expresidente británico, la empresa japonesa perdió más de US\$4,600 millones en capitalización de mercado.

Según la Fiscalía de Tokio, la empresa japonesa modificó en 2006 sus activos netos consolidados de 233.737 a 344.871 millones de yenes (de 2.252 a 3.324 millones de euros). En 2007 volvió a maquillar las cuentas para declarar 367.876 millones de yenes (3.545 millones de euros) cuando su valor real era de 254.246 millones de yenes (2.449 millones de euros).

Consecuencias

- La primera consecuencia fue un desplome de las cotizaciones de la firma en bolsa.
- La bolsa de valores de Tokio retiró la designación “valor bajo supervisión” por el de “valor en estado de alerta”.
- La empresa japonesa estuvo a punto de ser expulsada, en tanto no presentara sus estados financieros corregidos durante los cinco últimos años fiscales. Tras protagonizar este escándalo, se dañó la imagen de las corporaciones niponas.

ANEXOS

2.1 Procedimientos analíticos 1

Ejercicios de análisis de datos

Robo de efectivo

La línea de denuncia por presuntos fraudes de la organización recibió una llamada en donde se acusaba a Antonio, quien es gerente de contabilidad de la organización y quien en colusión con Sofía (una de sus subordinadas directas) han estado robando efectivo a la organización. De acuerdo con el informante, Sofía transfiere a su cuenta personal fondos en efectivo de los depósitos que se le encomiendan para depositar en el banco y Antonio manipula la contabilidad para cubrir el robo. El denunciante informa que incluso ambos mantienen una relación romántica, en contra de la política organizacional. Preocupado, el director de auditoría interna de la organización te solicita colaborar con la investigación debido a tus habilidades de análisis de datos.

Pregunta:

De los procedimientos y técnicas propuestas en el capítulo 2, ¿qué tipos de pruebas ejecutarías para ayudar a identificar si se ha perpetrado un fraude?

2.2 Procedimientos analíticos 2

Ejercicios de análisis de ratios

El caso gira en torno a una organización que se dedica al diseño y fabricación de electrodomésticos de alto nivel utilizando tecnología propia. Históricamente, la organización fue una división de otra organización y se separó de ésta en 2003.

Asimismo, ha invertido de manera importante en su nueva tecnología de 2002 a 2004 y se observa en sus estados financieros que:

- La introducción exitosa de sus productos en el mercado es la clave para su futuro.
- Si alcanza ventas significativas, deberá conseguir financiamiento adicional.

En noviembre de 2005, la organización inició una fusión inversa con otra de mayor tamaño pero privada. De acuerdo con el estado de ingresos para junio de 2006, se incluyen las actividades del negocio adquirido de diciembre 1 de 2005 a junio 30 de 2006.

En noviembre de 2006, la organización adquiere un proveedor de cámaras digitales, dando como resultado el aumento de plusvalía y activos intangibles reportados en 2007 en los estados financieros. Uno de los siguientes cinco fraudes han tenido lugar:

1. Fraude en los estados financieros antes de la fusión en el periodo 2002-2004, con el fin de hacer a la empresa más atractiva para la organización con la que se realiza la fusión.
2. Apropiación indebida de activos previa a la fusión, que fue realizada en algún momento entre 2002-2004 y reflejado en los estados financieros.
3. Fraude en los estados financieros posterior a la fusión entre 2005 y 2007 en los estados financieros.
4. Apropiación indebida de activos posterior a la fusión, que fue realizado entre 2005 y 2007 reflejado en los estados financieros.

5. Fraude en los estados financieros, perpetrado por la organización que fue comprada en noviembre de 2006 para obligar a la organización con la que se realiza la fusión a pagar más por la adquisición.

Su trabajo es aplicar el análisis de ratios y desarrollar una teoría acerca de cuál de los tipos de fraude tuvo lugar, observe el estado de resultados e ingresos y responda lo que se solicita a continuación.

Análisis preliminar

1. Basándose en los hechos que se plantean, ¿cuál es su teoría preliminar acerca del tipo de fraude que se realizó?
2. ¿De cuáles de los rubros del estado financiero se requeriría tener mayor información?
3. ¿Qué información adicional le ayudaría a realizar el análisis apropiado?
4. ¿Cuál es el mayor reto para desarrollar ratios realistas para esta organización?

Balance de ingresos						
(En miles de pesos)						
	2002	2003	2004	2005	2006	2007
Ventas netas	1,439	2,194	2,688	82,586	192,990	697,620
Costo de los bienes vendidos	12,869	9,829	13,047	71,825	169,096	573,155
Beneficio bruto	(11,430)	(7,635)	(10,359)	(10,761)	23,894	124,465
Gastos administrativos en ventas	3,333	4,890	3,671	10,417	26,443	52,260
Investigación y desarrollo	8,430	7,367	8,671	0	4,416	6,225
Cargos por devaluación	0	0	10,233	0	0	0
Ingresos/(pérdidas) por operaciones	(23,193)	(19,892)	(32,934)	334	(6,965)	65,980
Gastos por intereses	0	0	0	326	11,914	18,352
Otros ingresos/gastos	0	57	37	43	0	(21)
Ingreso antes de impuestos	(23,193)	(19,835)	(32,897)	61	(18,879)	47,607
Impuestos por ingresos	0	(1,091)	0	78	0	17,815
Ingreso neto/pérdida	(23,193)	(18,744)	(32,897)	(17)	(18,879)	29,792

	BALANCE GENERAL					
	2002	2003	2004	2005	2006	2007
Efectivo y equivalentes a efectivo	0	2,417	8,195	1,804	7,375	2,8679
Inversiones de corto plazo	0	12,000	13	0	0	0
Cuentas por cobrar	348	447	339	15,573	50,829	210,115
Inventario	2,584	2,735	5,400	15,139	13,151	34,499
Impuesto sobre la renta diferido	0	0	0	2,060	2,666	12,491
Otros activos corrientes	427	828	368	1,772	6,437	146,084
Total de activos corrientes	3,359	18,427	143,015	36,348	80,458	431,868
Propiedad y equipamiento	8,218	6,267	6,082	816	16,703	13,921
Inversiones de largo plazo	6,331	6,331	1,119	424	1,307	1,540
Bienes	0	0	0	0	6,990	30,546
Otros activos intangibles	9,527	8,768	0	0	20,737	36,413
Otros activos	0	0	0	46	1,461	377
Total de activos	27,535	39,793	21,516	37,634	127,656	514,665
Cuentas por pagar	516	457	1,230	9,287	3,924	71,563
Gastos acumulados	765	760	1,678	1,382	4,043	0
Notas por pagar	0	0	0	12,510	31,450	78,139
Ingresos diferidos	335	21	0	1,995	4,551	12,492
Impuestos por pagar sobre los ingresos	0	0	0	1,510	96	18,460
Otros pasivos corrientes	0	0	0	2,667	5,540	13,903
Total de pasivos corrientes	1,616	1,238	2,908	29,351	53,036	194,557
Deuda de largo plazo	0	0	0	0	3,758	0
Acciones preferidas redimibles	0	0	0	0	3,432	0
Impuestos sobre los ingresos diferidos	0	0	0	49	9,818	4,592
Total de pasivos	1,616	1,238	2,908	29,400	62,854	199,149
Capital contable	25,919	38,555	18,608	8,234	64,802	31,5518
Total de pasivos y capital contable	27,535	39,793	21,516	37,634	127,656	51,4565

Listado de soluciones para análisis de datos

- 130

4. AutoAudit
5. Arbutus Query
6. Dada Watch Corporation's Monarch para Windows
7. Micro Strategy Business Intelligence
8. Oversight Systems
9. Tableau Business Intelligence Software
10. SAP Crystal Reports
11. Oracle Business Intelligence Enterprise Edition Plus
12. SAS Enterprise BI Server
13. IBM Cognos 8 BI
14. Microsoft PowerPivot
15. TIBCO Spotfire Analytics

2.4 Entrevista e interrogatorio

Ejercicio de entrevista forense

Pedro comienza su procedimiento haciendo una revisión rápida a las cuentas por pagar. Ernesto Tompic es el jefe del área y ha trabajado para la organización por 20 años. Paulo Santos ha estado por seis años y Tadeo Blanco ha estado sólo tres meses en la organización.

Normalmente, cuando las facturas son recibidas, éstas son enviadas de inmediato a Paulo o Tadeo para su revisión. Ellos se aseguran de que las facturas están autorizadas y aprobadas por él en el departamento apropiado. Las facturas por encima de \$5,000 son enviadas a Ernesto para su aprobación final y luego se envían de vuelta a Paulo y Tadeo. Posterior a este paso se envía el cheque al proveedor.

Esta situación se discute con la gerente general financiera Cinthya Banks, quien mencionó que recientemente Juan Hernández se encarga de controlar la información y que le había informado que durante una revisión aleatoria de facturas, él encontró que muchas de ellas habían sido aprobadas solamente por Ernesto Tompic. Normalmente, éste sólo realiza una segunda aprobación en facturas por sobre \$5,000, pero nunca las aprueba. Juan Hernández preguntó a Ernesto Tompic acerca de estas facturas, pero Ernesto simplemente le dijo que desde que Tadeo inició en la organización, ha estado tratando de ayudarlo, aprobando las facturas por sí mismo sin tener que pasar primero por el filtro de Tadeo.

Un análisis de facturas pagadas durante los últimos 12 meses muestra que 40 facturas fueron aprobadas por Ernesto solamente, 15 de éstas fueron a una compañía llamada Industrias Cerdito. Una segunda investigación fue hecha a esta empresa y mostró que las 15 facturas que habían sido pagadas sumaban un total de 23,000 pesos.

Preguntas:

- ¿Debería Pedro comenzar a entrevistar en este momento o debería reunir información adicional? ¿Qué otra información se debe obtener?
- Elabore una lista de empleados que deberían ser entrevistados.
- Elija uno de ellos y elabore una guía de entrevista siguiendo los lineamientos generales de una entrevista para la investigación de fraude.

El principal objetivo del libro es ayudar a desarrollar a los jóvenes que están en las universidades a prepararse en el tema, necesitamos auditores forenses y mentes creativas con habilidades de investigación y substanciación, que tengan los conocimientos suficientes para prevenir y disuadir el fraude y, de igual manera, logren obtener el *Certified Fraud Examiner* (CFE) para ser reconocidos de manera internacional.

Desde nuestro IMCP y sus colegios federados tenemos el compromiso de aportar a nuestra sociedad y sus instituciones de conocimientos, es mi compromiso seguir aportando de mi tiempo con el objetivo de que este libro apoye en la construcción de una mejor sociedad.

Debemos procurar que nuestras organizaciones establezcan sus códigos de ética y conducta, una eficaz misión y visión; objetivos claros y concisos que todos los empleados los conozcan para crear conciencia y lealtad, lo cual nos ayuda a prevenir el fraude.

En un mundo cambiante en donde emerge el bitcoin por un mundo sin manejo de efectivo, las técnicas de auditoría forense son necesarias, y usar las tecnologías de información como una herramienta para combatirlo.

En 2017, México fue el segundo lugar con el mayor número de víctimas de fraude cibernético, con poco más de 33 millones de afectados, reveló un estudio de la empresa tecnológica estadounidense Norton; sólo Brasil lo superó con 62 millones de defraudados. El estudio estimó que los ciberdelincuentes robaron a clientes de servicios financieros, bancarios y empresas en México la cantidad de US\$7 700 000 000, principalmente porque los usuarios se comportan en internet de manera peligrosamente despreocupada. Lo anterior ocurrió por la infección de virus en computadoras y dispositivos móviles, seguidos del fraude en tarjetas de crédito, robo de contraseñas, hackeo de mail o cuenta de una red social y correos electrónicos fraudulentos. Otro rubro que creció de manera importante son las reclamaciones por posible fraude en comercio electrónico, pasando de 8% en 2011 a 49% en 2017.

Las líneas de denuncia son hoy un factor clave en los indicios de fraude, es importante que operen bajo tres bases de operación: anonimato, confidencialidad y seguridad. Como profesionales debemos de recomendar que las empresas públicas y privadas establezcan las líneas de denuncia que pueden ser contratadas de manera externa con compañías que ofrecen este servicio o de manera interna, aquí la reflexión importante que les dejo es: "¿Quién investigará las denuncias que lleguen por este medio y bajo qué parámetro serán realizados los filtros correspondientes?", esta pregunta podría ser tema de un nuevo libro.

En México, tanto el sistema nacional anticorrupción como los sistemas estatales anticorrupción crearán los comités de participación ciudadana, siendo la gran apuesta para que la ciudadanía pueda participar, actuar y opinar en estos temas; la auditoría forense y la auditoría de desempeño son las prácticas y técnicas que los profesionales del sector público y privado deberán complementar en su desarrollo profesional para tener un mejor país, así como instituciones y organizaciones inquebrantables que actúen con madurez y solidez ante los embates de la corrupción.

Tenemos que reconocer que al día de hoy vemos un marco de corrupción más organizado con temas como: fraude fiscal, peculado, delincuencia organizada y lavado de dinero.

En nuestro país es muy importante fortalecer a las autoridades en su labor investigadora y substanciadora para un mejor desempeño en el sistema nacional anticorrupción y los sistemas locales; para lo anterior, los perfiles forenses son clave en establecer una cultura antifraude.

La auditoría forense tiene que ser un tema del sector público; asimismo, tenemos que reconocer los avances que tienen las empresas privadas, pero habría que avanzar también en las compañías medianas y pequeñas y no que solamente los grandes conglomerados concentren esta técnica y conocimientos.

Otro aliado en nuestra lucha para combatir el fraude y la corrupción es sin duda alguna la norma ISO 37001, que es una certificación internacional en sistemas de gestión antisoborno, la cual nos ayudará con mecanismos efectivos a mitigar el riesgo del soborno y la corrupción, aplicándose en todo tipo de organizaciones (pública, privada y ONG) y en cualquier tipo de industria.

Esta norma ISO 37001 nos ayudará a crear una cultura antisoborno y será un distintivo que crea una ventaja competitiva y diferenciadora para las empresas y dependencias públicas. De igual manera, aplica un sistema de gestión contra el soborno, enfocado en la mejora y monitoreo continuo de los controles existentes.

Seamos optimistas, pues tenemos avances importantes en auditoría forense; espero que con este libro logremos mejores resultados en esta práctica, ya que el contexto internacional y nuestro país lo necesitan. Luchemos por mejores organizaciones y por profesionales de vanguardia. ¡Si podemos, pongamos juntos nuestro granito de arena, trabajando en equipo; sin envidias y con actitudes humildes y positivas lo lograremos!

- ACFE. (2016). *Fraud Examiners Manual*. Austin, Texas, USA.
- ACFE. (2016). *Report to the nations on occupational fraud and abuse*. Austin, USA.
- Commission, C. O. (2016). *Enterprise Risk Management: Aligning Risk with Strategy and Performance*. COSO.
- Cressey, D. (1972). *Criminal Organization: Its Elementary Forms*, Harper and Row, Nueva York.
- El Financiero*.
- Examiners, A. (2013). *Auditing/Investigating Fraud Seminar*. Las Vegas, USA. ACFE.
- Examiners, A. (2013). *Uncovering Fraud with Financial and Ratio Analysis*. Austin, Texas, USA. ACFE.
- G. Stevenson Smith, P. C. (2009). Defining a Forensic Audit. *Journal of Digital Forensics, Security and Law*.
- Informe Kroll (2015-2016). *Global fraud & risk report*. New York, EU.
- Nigrini, M. (2011). *Forensic Analytics*. New Jersey, USA: John Willey & Sons, Inc.
- Norton. (2014). *Informe de amenazas a la seguridad de internet*.
- Seminarios internacionales y nacionales de la ACFE*.
- SWGDE, Scientific Working Group on Digital Evidence. (2015). *Cibercriminalidad, fundamentos de investigación*, USA.
- The Institute of Internal Auditors. (2009). *GTAG Fraud Detection and Prevention*. Florida: The IIA.
- The Institute of Internal Auditors. (2012). *Glosario*. Florida: The IIA.
- Transparencia internacional*. (2016).
- Transparencia mexicana*. (2016).

Ilustración 1. Disciplinas relacionadas con la auditoría forense	18
Ilustración 2. Comparativo entre auditoría forense y otras disciplinas	19
Ilustración 3. Proceso de la auditoría forense.....	21
Ilustración 4. Árbol del fraude / Clasificación esquemas de fraude.....	22
Ilustración 5. Esquemas de fraude de robo de activos.....	24
Ilustración 6. Triángulo del fraude	28
Ilustración 7. Probabilidad de conducta ilícita o deshonesta	30
Ilustración 8. Diamante del fraude.....	30
Ilustración 9. Indicadores personales relacionados con el fraude	31
Ilustración 10. Indicadores de fraude por ciclo de negocio.....	33
Ilustración 11. Marco Integrado de Control COSO	37
Ilustración 12. Marco Integrado de Gestión de Riesgos Empresariales COSO-ERM.....	37
Ilustración 13. Cuadro comparativo de marcos de control.....	38
Ilustración 14. Proceso para evaluar riesgos y controles bajo el marco COSO.....	39
Ilustración 15. Marco integrado de control interno aplicado al fraude.....	42
Ilustración 16. Proceso para gestionar el riesgo de fraude	42
Ilustración 17. Frecuencia de existencia de controles antifraude.....	44
Ilustración 18. Debilidades de control que contribuyen al fraude	45
Ilustración 19. Esquema del sistema de gestión de riesgos.....	46
Ilustración 20. Métodos de detección de fraude ocupacional.....	49
Ilustración 21. Medios de denuncia	50
Ilustración 22. Fases de la auditoría forense.....	77
Ilustración 23. Evaluación del ambiente interno de fraude	78

Ilustración 24. Principales áreas de riesgo de fraude.....	79
Ilustración 25. Proceso de planeación de la auditoría forense.....	79
Ilustración 26. Ejecución de auditoría forense	81
Ilustración 27. Tipos de evidencia	81
Ilustración 28. Fases de la cadena de custodia	82
Ilustración 29. Inconsistencias en documentos de evidencia	84
Ilustración 30. Evaluación de la evidencia	84
Ilustración 31. Clasificación de procedimientos analíticos	92
Ilustración 32. Clasificación de la entrevista	97
Ilustración 33. Clasificación de la entrevista por tipo de preguntas.....	97
Ilustración 34. Proceso de interrogatorio	99
Ilustración 35. Fases del proceso dactiloscópico	106
Ilustración 36. Cronología del caso Supermercado Transnacional.....	112
Ilustración 37. Cronología del caso de la empresa Ingeniería Marina.....	117
Ilustración 38. Flujo de moneda digital y robo de información.....	123
Ilustración 39. Cronología del caso de la empresa de óptica e imagen	124
Ilustración 40. Evaluación del perfil de auditor forense.....	137
Ilustración 41. Estructura del laboratorio forense	145
Ilustración 42. Comparativo estadístico de fraude internacional.....	151
Ilustración 43. Ubicación geográfica de las víctimas de fraude	152
Ilustración 44. Frecuencia en los esquemas de fraude.....	153
Ilustración 45. Frecuencia de ocurrencia por esquema de fraude en América Latina y el Caribe.....	153
Ilustración 46. Índice de corrupción de acuerdo con el sector económico	154
Ilustración 47. Tipos de fraude más comunes en México.....	155
Ilustración 48. Corrupción en el sector público.....	155
Ilustración 49. Principales causas de la corrupción en México	156
Ilustración 50. Consecuencias de la corrupción.....	156